RIGA GRADUATE SCHOOL OF LAW

Comparative analysis of Latvian and Estonian AML requirements in regards to the virtual currency exchange service providers – theory and practice.

BACHELOR THESIS

AUTHOR: Niklāvs Tiļčiks

LL.B 2017/2018 year student
student number B017078

SUPERVISOR: *Ieva Rācenāja*
MBA

DECLARATION OF HONOUR:

I declare that this thesis is my own work, and that all references to, or quotations from, the work of others are fully and correctly cited.

(Signed)……

RIGA, 2020

ACKNOWLEDGMENTS

The author of this thesis expresses his deepest gratitude to Mrs Ieva Rācenāja for her assistance and support, while the thesis was conducted. Since the first interaction with the supervisor, periodic updates and feedback sessions pursued the author to polish the work until the desired level of accuracy was accomplished.

Furthermore, the author also is willing to express his deepest gratitude to the personnel of Riga Graduate School of Law, which throughout these years have created an inevitable interest to pursue in the field of financial crime, *e.g.* anti-money laundering.

As per concluding remarks - the last and most grateful "thank you" is devoted to the author's family, closest relatives and friends, which, regardless of experienced situations throughout three years, remained supportive and never originated second thoughts about their integrity, faith and utmost love.

Thank you.

ABSTRACT

Money laundering is considered as one of the most significant types of financial crime. Its magnitude has only increased in the past decade alongside with the development in the technological field. Since the regulatory framework seeks to mitigate threats posed by existing financial instruments, persons willing to initiate these actions still find new ways to proceed with illicit activities.

In that regard, this thesis focuses on comprehending regulatory scope and requirements governing virtual currency exchange service providers at the high level (European Union), while further analysis emphasises their implementation in Estonian and Latvian regulatory framework. By comprehending minimum requirements set in respective legal systems, in-depth analysis and further comparison will highlight differences, which arises between regulatory attitudes towards these service providers stemming from both member states of the EU.

Since virtual currency as such has been legally defined only by the 5th anti-money laundering directive, the regulatory application remains uncertain, therefore theoretical and practical analysis, thus comparison seeks to comprehend different approaches considered by respective jurisdictions.

Key words: AML, virtual currency exchange service providers, compliance, virtual currency, fiat currency.

SUMMARY

During the past decade, money laundering has exposed and created a majority of threats to the global financial system. Criminals, nowadays, tend to use different types of complex schemes in order to integrate illicitly obtained funds into both local and international financial sector. By comprehending contemporary financial technology solutions, their activities have become even more sophisticated, thus dangerous.

One of such financial technology is crypto or virtual currency. Since virtual currencies have created a huge resonant in the society, their regulatory scope has also developed alongside the financial technology itself.

The author's objected thesis "Comparative analysis of Latvian and Estonian AML requirements in regards to the virtual currency exchange service providers – theory and practice" aims to comprehend minimum requirements set in Latvian and Estonian respective AML laws, which, mainly, derives from 4th and 5th AML directive.

The scope of this thesis respects virtual currency exchange service providers in light of the AML requirements set in an international and local level. As per it was mentioned, only virtual currency exchange service providers and their applicable legal norms will be analysed, thus limiting the author to the researchable amount of information. In the thesis itself, whenever the author mentions "virtual currency service providers" in particular form and wording, it should be perceived as the "virtual currency exchange service providers" instead. Among other things - since virtual currency topic, in general, is also related to complex taxation matters, this thesis will only emphasize and focus on requirements stemming from the AML point of view, thus avoiding any involvement of said additional provisions.

The author of this thesis has divided the work into three separate chapters, whereas each chapter will supplement the next one and vice versa.

The first chapter serves the purpose of introducing the reader with the rationale and cruciality of the AML by considering both international and national perspective. The whole chapter consists of descriptive and analytical elements, which touches upon the history of the virtual currencies as such and also seeks to identify key defining elements, which corresponds to the concept of the AML. Such correlation seeks to give a basic insight into what the AML essentially is and how virtual currencies have evolved during the past years.

The second chapter elaborates and seeks to comprehend regulatory requirements set in Latvian and Estonian legal framework in regards to the virtual currency service providers. The emphasis is put on comprehending practical deficiencies stemming from regulatory requirements, which have been compared to the best industry practice adopted in the EU and elsewhere. By understanding how practically these requirements could be applied to the virtual currency exchange service providers, the author can establish ground fundamental for further comparison and additional analysis. Also, both legal and economic perspective will be comprehended since compliance, in general, is a very costly mechanism, which supplements institutions internal safeguarding systems.

The third chapter consists of a legal and economic comparison between Latvian AML law minimum requirements and Estonian AML law minimum requirements. This comparison

is perceived by creating a fictitious scenario whereas the company X has to decide which market would be most suitable for desired virtual currency operations.

In conclusion, the thesis summarizes and gives an overview of what has been discovered during the research phase. As per understanding the practical application stemming from minimum requirements set in both jurisdiction legal systems, the author gives an overall evaluation of whether these requirements fulfil their objectives by collecting and analysing the evidence throughout the whole paper. The second part of the conclusion analyses, which of both jurisdictions is more beneficial to operate the virtual currency business. By analysing both legal and economic factors, the comprehensive overview clarifies aforementioned.

TABLE OF CONTENTS

INTRODUCTION

> Money laundering is a difficult crime to detect. Its consequences can have a severe impact on the EU's economy and on its financial system. Therefore, the EU needs to have a multi-faceted approach to properly tackle money laundering and terrorist financing. Action is needed on several levels.[1]

As it is stipulated in the provided quote, money laundering indeed is a serious threat, which currently seeks to infiltrate and thus cripple the financial sector. Legislators for years have tried their best in order to mitigate the flow of illegally obtained funds. By introducing the first AML directive in 1990[2], primordial incentives can be already detected – common thought of combating financial crime was quite important in order to maintain an integrity and trustworthiness of the EU's financial sector.

Having said that, it must be noted that primordial requirements, although were designated to prevent financial crime, in majority of cases played only a formal, rule-based role[3] due to the fact that risk based approach occurred only alongside the 3rd/4th AML directive[4]. Eventually, such risk based approach underlines several concepts and subsequent principles, which allows particular subjects of the law to ensure higher and stricter compliance standards.

Nevertheless, previously mentioned risk based approach allows institutions to face and tolerate higher risk, therefore extension of business scope by establishing new relationships is more likely to occur. This, however, rises concerns, whether new relationships comes in addition with new technological channel risk, for instance. As per elaborating on that thought, one of the recent technological trend touches upon the concept of virtual currencies, their users and their providers. The incentives to regulate this particular sphere on the EU level can be already found in 2012[5] whereas the European Central Bank issued a report indicating how uncertain and risk possessing such instrument can be. However, due to the rapid technological development, which also is reinforced by the society's willingness to try out unexperienced things, virtual currencies as such gradually gained popularity[6] among particular groups of people by becoming as an ordinary, supplementary thing.

By understanding that virtual currencies indeed becomes more and more used in people daily lives, regulatory action was necessary in order to sustain a safe financial environment and mitigate unregulated threat exposure, which thrived by using particular instrument/asset[7]. By introducing the AML 5th directive, the EU as one of the subject of the

---

[1] European Commission, Questions and Answers – Commission steps up fight against money laundering and terrorist financing, 07.05.2020, Available at https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_821, Accessed on 13.05.2020.

[2] European Commission, Anti-money laundering and counter terrorist financing, 19 July 2018, Available at https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-counter-terrorist-financing_en, Accessed on 13.05.2020.

[3] Paolo Costanzo, Rule – Based Vs. Risk – Based Approaches to Control. The Third EU Anti – Money Laundering
Directive, Utrecht School of Economics, 03.11.2007, p. 1, Available at http://www2.econ.uu.nl/users/unger/papers/Costanzo.pdf , Accessed on 13.05.2020.

[4] *Ibid.*

[5] *Infra* note 63.

[6] *Infra* note 79.

[7] *Infra* note 47.

law, made a virtual currency service providers. This, however, posed an obligation to the member states to integrate particular provision in respective legal systems.

Eventually, since the member states are required to be compliant with the directive and given the fact that virtual currencies in general are something relatively new, different approach for regulating them was expected to occur, therefore, in order to comprehend different attitude towards these service provider, the author of this thesis selected two in theory similar jurisdictions and analyzed their minimum requirements stemming from the AML law in regards to the virtual currency exchange service providers.

This however already establishes primordial thoughts of potential differences that may arise since the interpretation is left to the each member state and that would, eventually, rely on underlined risk perception, which has been tolerated considering national risk assessment.

Moreover, respective requirements can be found in the Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing (Latvia) and in the Money Laundering and Terrorist Financing Prevention Act (Estonia).

Methodology

The author of this thesis used qualitative comparative analysis in order to comprehend the requirements set in Latvian and Estonian AML law in regards to the virtual currency exchange service providers. As for the first part of the thesis, also grammatical interpretation method was used in order to comprehend the scope of the virtual currency service providers introduced by the AML 5th directive. Further analysis, however was based on previously mentioned comparative analysis by analyzing legal acts, regulatory guidelines issued by local and international authorities. Additionally secondary sources such as reports, opinions and clarifications reinforced the arguments provided in the thesis.

Research Questions:

1. To what extent minimum requirements set in Latvian and Estonian AML law are attributable to the virtual currency exchange service providers?
2. Which of the abovementioned jurisdictions provides more beneficial environment to operate a virtual currency exchange service requirement business?

1. KEY PRINCIPLES AND CONCEPTS OF THE ANTI-MONEY LAUNDERING AS A SET OF LAWS AND REGULATORY REQUIREMENTS

Not only the European Union (hereinafter referred to as the "EU") but also the rest of the world has declared and recognized the importance of money laundering (hereinafter referred to as the "ML") as an issue, which emerges and develops within the changes in regulatory framework. These changes, however, seeks to robust current legislative framework and comprehension by clarifying and thus mitigating options for criminals to avoid laws in order to funnel state's financial sector with illicitly obtained funds. By passing new and more strict binding rules, the EU, for instance, seeks to protect its financial sector's integrity by promoting good governance[8], therefore posing an obligation to its member states (hereinafter referred to as the "MS") to ensure transparency and enhanced monitoring over its financial institutions[9]. This chapter, on the other hand, will be devoted for describing, but mainly analyzing key principles and concepts of the AML in relation to internationally adopted the best practice principles.

1.1. Rationale behind the concept of the AML

As it was mentioned beforehand, the EU in particular, drives its forces towards achieving financial integrity and sector transparency by providing and adopting new set of procedures, guidelines, recommendations and decisions to the MS to be compliant with. This compliance, however, poses a huge burden of issues[10], which remains delusional by reason that regulation is effective until the extent when it remains on paper.

As it is observable currently, financial institutions struggles to maintain utmost compliance since adopted requirements are compatible and complex set of mechanisms. For instance, in 2018 Latvia proposed set of new requirements to mitigate AML threats due to the non-resident proportion having accounts in Latvian banks[11]. However non-residents turned out to be a huge deal since aggregate deposited amount of money accumulated up to 30% per year[12]. Such tranche, on the other hand, was satisfying for local bankers and incentives, thus provided services designed for non-residents, kept expanding by tolerating more and more risky customers. One of the major Latvian private bank ABLV got its license withdrawn by the European Central Bank[13] (hereinafter referred to as the "ECB") due to the commentary released by the Financial Crimes Enforcement Network (hereinafter referred to as the "FinCEN"), which established that

[8] International Monetary Fund, Assessing Financial System Integrity—Anti-Money Laundering and Combating the Financing of Terrorism, Financial Sector Assessment: A Handbook, Chapter 8, p. 207, Available at https://www.imf.org/external/pubs/ft/fsa/eng/pdf/ch08.pdf, Accessed on 05.04.2020.
[9] *Ibid.*
[10] Thomson Reuters, 5 questions that can help reduce the regulatory burden on compliance officers, Available at https://legal.thomsonreuters.com/en/insights/articles/reducing-regulatory-burden-on-compliance-officers Accessed on 05.04.2020.
[11] Joshua Kirschenbaum, German Marshall Fund of the United States, Report, 2018, Available at www.jstor.org/stable/resrep18827, Accessed on 05.04.2020.
[12] *Ibid*, p. 2.
[13] Pēters Putniņš, ABLV Bank AS licence ir anulēta, bankas pašlikvidācija norit FKTK uzraudzībā, FKTK, 12.07.2018, Available at https://www.fktk.lv/jaunumi/pazinojumi-medijiem/peters-putnins-ablv-bank-as-licence-ir-anuleta-bankas-paslikvidacija-norit-fktk-uzraudziba/, Accessed on 05.04.2020

> [...] ABLV has institutionalized money laundering as a pillar of the bank's business practices. ABLV's management permits the bank and its employees to orchestrate money laundering schemes; solicits high-risk shell company activity that enables the bank and its customers to launder funds; maintains inadequate controls over high-risk shell company accounts; and seeks to obstruct enforcement of Latvian anti-money laundering and combating the financing of terrorism (AML/CFT) rules in order to protect these business practices[14]

The commentary showed that AML as set of risk mitigation mechanisms, is taken seriously not only EU-wise, but also reflects further over the ocean. Since such notice was unexpected not only to the Bank itself but also to the supervisory authority Financial and Capital Market Commission (hereinafter referred to as the "FCMC"), escalated actions resulted in a self-liquidation process in which the bank is currently involved.

1.2. Key defining elements of the AML

As per described previously, AML has been recognized as an integrity driving concept world-widely. However, before going into detail, it is necessary to define key elements, which are crucial in perceiving the concept fully. For the purposes of this section's examination, the author of this work introduces three key elements, which defines the core concept of the AML. After having listed them, further analysis will reinforce their crucially by providing examples how aforementioned fits into legislative understanding.

1.2.1. Identification

The first defining element is an identification. Identification, hence, goes hand in hand with the principles set in the customer due diligence (hereinafter referred to as the "CDD") requirements. 3rd AML Directive[15], conceptually, introduced the KYC/CDD requirement in the Article 8, providing the following,

> Customer due diligence measures shall comprise:
>
> (a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;
>
> (b) identifying, where applicable, the beneficial owner and taking risk-based and adequate measures to verify his identity so that the institution or person covered by this Directive is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts and similar legal arrangements, taking risk-based and adequate measures to understand the ownership and control structure of the customer; [...][16]

By comprehending the quoted text, it is possible to drive a conclusion that CDD measures are highly necessary for establishing an overall understanding of who the customer is. After having conducted the identification process, the subject of the law creates a

[14] Steve Hudak, FinCEN Names ABLV Bank of Latvia an Institution of Primary Money Laundering Concern and Proposes Section 311 Special Measure, 13.02.2018, Available at https://www.fincen.gov/news/news-releases/fincen-names-ablv-bank-latvia-institution-primary-money-laundering-concern-and, Accessed on 05.04.2020

[15] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

[16] *Ibid*, Article 8.

primordial comprehension of the possible arising risks and the nature of the expected relationship. Financial Action Task Force's (hereinafter referred to as the "FATF") recommendation Nr. 10[17] specifically addresses this issue by forbidding to maintain business relations with the anonymous account holders[18]. Due to this principal's significant implication, the author of this work purses identification as on the defining element of the whole AML concept.

1.2.2. Transparency

As for the second key element, the author of this work highly emphasizes Commission's incentives to establish an EU-wide transparency[19] framework within its internal market, therefore transparency as a key element will be analyzed further in this subsection. Transparency has two natures - global and internal, whereas both causes each other.

Transparency, although should be perceived as a different topic, goes hand in hand with the aforementioned in a line that identification as such ensures further traceability of customer's funds, which eventually means a transparent operations in the bank account. This, however, should be perceived as an internal transparency due to the fact that it occurs between a subject of the law and the customer. European Banking Authority (hereinafter referred to as the "EBA") emphasizes that "Firms should ensure that their approach to transaction monitoring is effective and appropriate"[20]. By recycling the aforementioned, the credit institutions are required by the law to implement effective set of procedures and processes governing transaction monitoring for the purposes of ensuring transparency and compliance with the law within the financial institution.

As it was mentioned in the beginning, the transparency as such can be divided in two separate categories - global and internal. By clarifying, what in the author's opinion should be understood as an internal transparency, the global one goes hand in hand with it.

Whilst internal transparency occurs within the institution, the global one is highly affected by the compliance results of the first one. For instance, let us suppose, that the state A is the MS of the EU. All the regulatory requirements are binding and for the purposes of this example - transposed into the national legislation. State's A supervisory authority has been instructed by the EU to closely monitor its financial sector and participating credit institutions. If, for instance, participating credit institutions are not being compliant with the law, assessment of their performance in the field of ML will be evaluated as low, thus receiving a negative result in compliance assessment.

[17] International Standards On Combating Money Laundering and The Financing of Terrorism & Proliferation The FATF Recommendations updated June 2019, Recommendation No. 10
[18] *Ibid*, p. 12.
[19] Sophie van Bijsterveld, Section 5, Transparency In The European Union: A Crucial Link In Shaping The New Social Contract Between The Citizen And The Eu, Available at https://www.ip-rs.si/fileadmin/user_upload/Pdf/clanki/Agenda__Bijsterveld-Paper.pdf Accessed on 05.04.2020.
[20] Draft Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (''The Risk Factors Guidelines''), amending Guidelines JC/2017/37 TRANSACTION MONITOIRNG Accessed on 05.04.2020.

Mentioned transparency, on the other hand, underlines risks, which emerges, if appropriate set of mitigating controls have not been tolerated adequately[21]. Risks, such as reputational and financial can occur unexpectedly, therefore, in order to maintain sound management over the institution, it necessary to implement straightforward and concise guidelines[22], which governs overall approach in governing daily operations of the said institution.

1.2.3. Risk based approach

Having said aforementioned, the third defining AML element is risk-based approach[23] (hereinafter referred to as the "RBA"). By comprehending this term, it is crucial to firstly define what the risk is, thus according to the report issued by the World Bank, the term risk defines "the combination of the likelihood of an adverse event (hazard, harm) occurring, and of the potential magnitude of the damage caused (itself combining number of people affected, and severity of the damage for each)"[24]. As per the definition provided by the World Bank, it is duly perceivable that risk contains set of adverse events and potential consequences. European Commission, on the other hand, reinforces the term risk, by dividing two separate variables - hazard[25] and risk[26] and therefore stipulates the following

> A hazard is any source of potential damage, harm or adverse effects on something (*e.g.* the environment) or someone. Risk is the chance or probability that a person or something will be harmed or experience an adverse effect if exposed to a hazard.[27]

Hereby, in relation to the ML, Article 1, subparagraph 1.1 of the FCMC's provision Nr.3 (which is not in force anymore), defines risk as "[...] the impact and probability that a credit institution may be used in money laundering or terrorism financing"[28].

As it is observable, all provided explanations seeks to follow a single common denominator - there has to be an occurrence of an event, which demonstrates within itself an element of threat or incident, which, eventually, reinforces threats towards a particular

---

[21] EY, Why financial institutions need to focus on transparency, 12.07.2019, Available at https://www.ey.com/en_om/tax/why-financial-institutions-need-to-focus-on-transparency Accessed on 05.04.2020.

[22] Mckinsey&Company, Why anti-money laundering should be top priority for financial institutions, Available at https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/banking%20blog/why%20aml%20should%20be%20a%20top%20priority%20for%20financial%20institutions/why-aml-should-be-a-top-priority-for-financial-institutions.ashx, Accessed on 05.04.2020.

[23] Zhang Fan, The "Risk-Based" Principle of AML Management, 19.09.2017, Available at https://www.acamstoday.org/the-risk-based-principle-of-aml-management/, Accessed on 05.04.2020.

[24] Florentin Blanc, Ernesto Franco-Temple, Introducing a risk-based approach to regulate businesses, how to build a risk matrix to classify enterprises or activities, Nuts & bolts. Washington, DC, World Bank Group, 2013, Available at http://documents.worldbank.org/curated/en/102431468152704305/Introducing-a-risk-based-approach-to-regulate-businesses-how-to-build-a-risk-matrix-to-classify-enterprises-or-activities, Accessed on 05.04.2020.

[25] European Commission, What Is Hazard And Risk, Risk Assessment And Management, Available at https://ec.europa.eu/info/sites/info/files/file_import/better-regulation-toolbox-15_en_0.pdf, Accessed on 06.04.2020.

[26] *Ibid.*

[27] *Ibid*, What Is Hazard and Risk.

[28] Section 1.1., Finanšu un kapitāla tirgus komisijas 2018. gada 9. janvāra noteikumi Nr. 3 "Klientu padziļinātās izpētes normatīvie noteikumi kredītiestādēm un licencētām maksājumu un elektroniskās naudas iestādēm". Latvijas Vēstnesis, 10, 15.01.2018, Available at https://likumi.lv/ta/id/296439/redakcijas-datums/2018/06/02. Accessed on 06.04.2020.

subject. In relation to the subject matter, endangered subjects can be both - involved persons in the ML activities itself, and negatively affected financial institutions, which, as a matter of an opinion, can also be considered as involved persons, if the harm has been done intentionally.

After having defined the first essential element of the RBA, proceeding clarifications seeks to establish an environment for parallels between the AML and RBA, where concept is developed by introducing mutual correlation as a tool, which is used to combat ML.

Financial Action Task Force (hereinafter referred to as the "FATF") has passed multiple guidelines and recommendations for both MS and financial institutions in order to more efficiently mitigate and identify ML posed risks[29] and to the extent possible - avoid potential involvement of being engaged in the ML and sanctions violation schemes[30] directly or indirectly. Considering RBA as one of defining elements for the concept of AML, the FATF, moreover, throughout its report "Guidance of a risk-based approach. The Banking Sector., October 2014"[31] emphasizes the need to tolerate risk, using RBA for the purposes of establishing a risk assessment system, which must assign the corresponding level of risk for each of the financial institution's customer[32]. This provision, on the other hand, also consists of the necessity to perceive possible both residual and inherited risks, which might affect the institution's credibility, reputation and operability in the market[33]. In practice, the aforementioned numerical risk assessment is transposed into the scoring system, which determines two aspects - level of the risk and precise score thriving from the assigned level. For the purposes of establishing a fundamental clarity, the author by using the best international industry practice will elaborate on the practical rationale behind the scoring system.

There are 6 possible levels of risk - very low, low, medium, high, very high[34] and the level exceeding "very high" is considered as a zero-tolerance policy threshold, where customers accumulating such score are automatically prohibited to open an account to further operate in the financial system with their funds by reason of exposing risks, which are contrary to the institution's risk appetite.

Nevertheless, after establishing what the levels of risk are, each of them consists of certain numerical margins whereas each category is assignable after considering different circumstances and scenarios adopted by the financial institution. Let's imagine, that the institution has set the following margins as:

- 1-10 corresponds to the very low risk
- 11-25 corresponds to the low risk
- 26-51 corresponds to the medium risk
- 51-78 corresponds to the high risk

[29] FATF, Who we are, Available at https://www.fatf-gafi.org/about/ , Accessed on 06.04.2020.
[30] *Ibid*
[31] FATF, Guidance for A Risk-Based Approach, The Banking Sector, 2014, Available at http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf, Accessed on 07.04.2020.
[32] *Ibid*, Assessing ML/TF Risk, p. 9.
[33] *Ibid.*
[34] *Ibid*, Germany, p. 28.

- 79-100 corresponds to the very high risk
- >100 corresponds to the prohibition to open a bank account for the customer.

The particular scoring for a customer is generated by comprehending different scenarios provided by both national supervisory authority (FCMC in Latvia, the Bank of Lithuania in Lithuania, *etc*.), and international safeguard/watchdog (the FATF, the EBA, *etc*.). These scenarios are created in a way, that financial institutions are free to determine applicable risk score for particular factor, for instance, in the latest commentary[35] passed by the EBA, several question-related factors[36] have been introduced, which seeks to clarify the business nature of the customer, thus reinforcing the KYC principles. Furthermore - as it was clarified previously, the risk score is generated by summing accumulated risk factors, for instance, the risk factor stipulates that increased customer risk occurs if the customer or related person is a politically exposed person (hereinafter referred to as the "PEP")[37]. In such case, financial institution is responsible for assigning a risk score considering inherited risk exposure[38]. If, for instance, the institution seeks to score such factor by 10 points, it means, that whenever a customer will have an applicable PEP factor, it automatically will receive 10 points to his/her aggregate risks assessment. And by scoring each of implemented ML risk factor, the institution will have a comprehensive risk scoring system assigning particular scores for particular customers whereas, eventually, the RBA has been used as a tool to mitigate potential involvement in the ML schemes and, thus reinforcing and transposing AML core values and driving incentives in a material format.

Regardless of the previously mentioned example, the RBA is also used in order to determine financial institution's risk appetite (by also applying enterprise wide risk assessment[39] (hereinafter referred to as the "EWRA")), tone from the top, risk mitigation strategy.

1.3. Historical background of virtual currencies

Due to the nature of this paper and prior conducting an extensive legal analysis, the author of this paper seeks to establish the fundamental background to understand how the virtual

[35] EBA, Consultation paper, Draft Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (''The Risk Factors Guidelines''), amending Guidelines JC/2017/37, 5 February 2020, Available at https://eba.europa.eu/sites/default/documents/files/document_library/Publications/Consultations/2020/Draft%20Guidelines%20under%20Articles%2017%20and%2018%284%29%20of%20Directive%20%28EU%29%202015/849%20on%20customer/JC%202019%2087%20CP%20on%20draft%20GL%20on%20MLTF%20risk%20factors.pdf, Accessed on 08.04.2020.

[36] *Ibid.*

[37] Appendix 1, Risk factor No. 4., Finanšu un kapitāla tirgus komisijas 2019. gada 21. augusta noteikumi Nr. 135 "Klientu izpētes, klientu padziļinātās izpētes un skaitliskā riska novērtējuma sistēmas izveides normatīvie noteikumi". Latvijas Vēstnesis, 176, 29.08.2019. https://likumi.lv/ta/id/309047, Accessed on 08.04.2020.

[38] The Wolfsberg Group, Appendix C: Example Client Inherent Risk Ratings, The Wolfsberg Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption, Available at https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/faqs/17.%20Wolfsberg-Risk-Assessment-FAQs-2015.pdf, Accessed on 08.04.2020.

[39] *Supra*, note 35, p. 29, 1.18.

currencies are treated in the EU framework, how they must be perceived and what are the key aspects, which makes them as an opaque financial instrument in regards to comprehension from the AML perspective.

Since the rapid development in popularity of this financial instrument, it has exposed new and complex threats and risks[40] of how it can be used for illegitimate reasons. If, for instance, 5 years ago majority of people were not aware that such financial instrument as virtual currencies exists[41], nowadays the portion of people who have heard something about virtual currencies is far greater than it was previously. As per their failure to become as a sovereign payment method[42], virtual currencies, stimulated by their decentralization, have turned to be appealing and attractive for terrorists[43] in order to maintain their activities possible. To establish greater clarity - large or relatively large terrorist organizations are not relying on financing their operations by using virtual currencies due to the unpredictable volatility[44] and instability[45], although these type of financial instruments are mostly used by so called lone wolfs[4647] in considerably younger age since their comprehension and skills in technological sphere are far more advanced than older generation has.

1.3.1. Driving incentives for regulating virtual currencies

In order to even perceive key factors, which were at the time remarkable and sufficient enough to establish primordial incentives to regulate this particular niche, the author of this work is willing to set aligned definition of what virtual currencies are and what are driving differences, which separates it from other type of financial instrument.

Prior the 5th AML directive being issued, there was no legal and unified term of what virtual currencies or crypto currencies are. Each watchdog had introduced its own definition of what these financial instruments might be considered as[48], by basing their opinions on surrounding specific circumstances and scope of work. The FATF has its own definition, which was similar but with minor differences to one, which was established by the EBA, for instance, therefore such distinction created a regulatory loophole and gap where conceptual comprehension existed, while practical approach and practice was not yet established.

---

[40] Tobias Adrian, Tommaso Mancini Griffoli, The rise of digital money, International Monetary Fund 2019, 15.07.2019, p. 6, Available at https://www.imf.org/en/Publications/fintech-notes/Issues/2019/07/12/The-Rise-of-Digital-Money-47097, Accessed on 08.04.2020.

[41] The statement can be made by considering the change in price 5 years ago and now, since virtual curencies are worth what their traders assign them.

[42] Morten Bech, Rodney Garratt, Central bank cryptocurrencies, BIS Quarterly Review, September 2017 Available at https://www.bis.org/publ/qtrpdf/r_qt1709f.pdf, Accessed on 09.04.2020.

[43] European Parliament, Virtual currencies and terrorist financing: assessing the risks and evaluating responses, p. 27, Available at https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf , Accessed on 08.04.2020

[44] *Ibid*, p. 28.

[45] *Ibid.*

[46] Lone wolf terrorist attacks occurs when a single person regardless of his/her attribution to a certain organisation/religion, executes attacks with the purpose to negatively influence persosn surrounding him/her.

[47] *Supra*, note 43, p. 28.

[48] European Parliament, Cryptocurrencies and Blockchain, Legal context and implications for financial crime, money laundering and tax evasion, p. 20-22, Available at https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf , Accessed 10.04.2020.

Nevertheless, as per defined by the European Commission in the AML 5th Directive[49], amendments made in the Article 3, by introducing the term "virtual currencies" stipulates that,

> "virtual currencies" means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically[50]

The introduction of such term has been explained in the preamble of the said directive, specifically in recital Nr. 9, which demonstrates that "[t]he anonymity of virtual currencies allows their potential misuse for criminal purposes"[51]. Thus as it is perceivable, the first emerging issue touches upon the failure to avoid anonymity whilst these financial instruments are used.

As for the second determining issue, the author of this work points out the distinction made by the FATF in 2014 between centralized and decentralized virtual currencies.[52] As it is stipulated in the report, centralized virtual currencies have issuing and administrative authority, which maintains, regulates and passes rules and guidelines of what can and what cannot be done with this type of currency[53], whilst decentralized virtual currencies, such as bitcoin, does not have specific characteristics of a currency, nor it has a backed value[54], nor it has an administrative authority[55]. As being pointed out as a second concern, emphasized methodological problem creates a breakthrough for the ML to occur due to the lack of the EU-wide regulatory framework, which was not developed at the time back then.

By having identified two main concerns, which underlines possible threats in relation to the ML, the author of this work seeks to establish last element, which poses challenges in relation to legal framework - technological complexity[56]. For the purposes of clarifying technological rationale behind virtual currencies, derivative - cryptocurrency as well as supplementing blockchain will be taken as reference point to establish a case.

According to the European Commission, blockchain is

> [...] a technology that allows people and organizations to reach agreement on and permanently record transactions and information in a transparent way without a central authority. It has been recognized as an important tool for building a fair, inclusive, secure and democratic digital economy [...].[57]

---

[49] DIRECTIVE (EU) 2018/843 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.
[50] *Ibid*, Article 3, Paragraph (d).
[51] *Ibid*, Recital 9.
[52] FATF, Virtual Currencies, Key Definitions and, Potential AML/CFT Risks, June 2014, Available at https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, Accessed on 10.04.2020.
[53] *Ibid*, p. 5
[54] *Supra* note 48, p. 23, Summary.
[55] *Ibid*, p. 5.
[56] Simon Dyson, William J Buchanan, Liam Bell, The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime, 29.07.2019, p. 2 , Available at https://arxiv.org/pdf/1907.12221.pdf , Accessed 11.04.2020.
[57]European Commission, Blockchain Technologies, 15 January 2020, Available at https://ec.europa.eu/digital-single-market/en/blockchain-technologies, Accessed on 12.04.2020.

However this definition is not comprehensible enough due to its "positive nature". Key concerns, which arises from the blockchain, touches upon the anonymity/pseidoanonimity[58] and lack of determinable liability involved in the transaction between the parties[59]. Nevertheless, due to the fact that blockchain is a form of distributed ledger technology[60], there have been incentives to put a regulatory framework over this technological concept.

Aforementioned regulatory framework could be imposed on the blockchain, if its legal status would be recognized. This, however, seeks to have an identification for related functions, which should be taken into account prior recognizing ones status. "[...] logging and time stamping of transactions, linked recording and digital signing, cryptography, access and permission, digital identity, consensus algorithms"[61] - these functions are cumulatively integrated in the blockchain[62] and defines its complex nature. Although they are not new and can be found already as working tools, some of these functions can be regulated by the Regulation Nr. L 257/73 on electronic identification and trust services for electronic transactions in the internal market[63].

The key concern, which forbids recognizing blockhain's legal status is that there is a relative and practical unavailability to impose liability claims on involved parties[64] as well as blockchain could not be recognized as Trust Service Provider (hereinafter referred to as the "TSP") since it lacks full scope of signatory integrity.

As per having identified three main concerns, which emerges from the virtual currencies, the author of this work has clarified what are the main circumstances pushing regulatory framework towards complete compliance, however, on the other hand, the author can already draw a conclusion, that these financial instruments, regardless of their novelty, constitutes set of complex principles and mechanisms, which are merely impossible to comprehend and efficiently regulate on a practical basis. Underlined risk exposures are not genuinely manageable, therefore adopted incentives to regulate this particular technological solution may work in the theory, since the financial sector have just understood legal requirements set in the AML 5th directive. Such rapid development in the legislative framework means high level adoption and alignment, thus in-depth notion may not even appear as it was expected.

[58] The European Union Blockchain Observatory And Forum, Legal And Regulatory Framework Of Blockchains And Smart Contracts, Available at https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf , Accessed 12.04.2020.
[59] *Ibid*, p. 6.
[60] OECD, The Policy Environment for Blockchain Innovation and Adoption 2019 OECD Global Blockchain Policy Forum Summary Report, Available at https://www.oecd.org/finance/2019-OECD-Global-Blockchain-Policy-Forum-Summary-Report.pdf, Accessed on 13.04.2020.
[61] EU-LISA, Perspectives for EU-LISA and the Large-scale IT Systems, Research and Technology Monitoring Report, 2019, Available at https://www.eulisa.europa.eu/Publications/Reports/DLTs%20and%20blockchain%20report.%20Dec%202019.pdf , Accessed 12.04.2020.
[62] *Ibid*, p. 4.
[63] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
[64] *Supra*, note 58, p. 12.

1.3.2. Development of the regulatory framework in the EU and Latvian context

As it was discussed previously, defined regulatory requirements governing virtual currencies appeared only when the 5th AML directive was passed and, thus came in force. Beforehand there was a lack of equivalent regulation since a hectic and even holistic approach was implied.

1.3.2.1. The EU-wide context

In order to comprehend the existing development of regulatory framework regarding virtual currencies on a national (Latvian) scale, it is necessary to analyses and discerns EU-wide aligned approach for determining what are the components and familiar elements of cryptocurrencies or virtual currencies.

Among the other things, one of the first EU-wide sub-legal discussions surrounding virtual currencies can be found already in 2012, when the European Central Bank (hereinafter referred to as the "ECB") issued a report on virtual currencies schemes (October 2012)[65] stipulation opinions of what virtual currencies are, what are their potential implications to the financial sector and what are the potential issues emerging from the usage of said[66]. The author of this work does not recognize nor establishes the fact that this particular report serves the basis for regulating cryptocurrencies or virtual currencies, in contrary - it ought to be perceived as one of the first issued reports by the supervisory authority for the purposes of clarifying certain specific questions/concerns.

Already in 2012 it has been acknowledged that virtual currencies as means of payment exists and can have a futuristic impact on the sector and understanding of what money is and what might be the next big tendencies in its regard. Eventually, the issued report created a fertile soil for building opinion-based non-binding resolutions, which clarified recent tendencies and key issues concerning the usage of virtual currencies.

Prior to this report, however, certain MS recognized virtual currencies as a means of payment. For instance, although one year later in 2013, Germany, under German Banking Act, by classifying virtual currencies as financial instruments[67], recognized such possibility to conduct a transaction, whereas virtual currencies are involved. German supervisory authority recognized that by using this decentralized payment method, involved parties essentially shares the same characteristics as it would be in the case of having an exchange of goods by involving money as perceived in the common context[68]. Earlier, already in 2011, France had held discussions arguing, addressing and rising concerns about digital currencies possible involvement in the ML and terrorist financing schemes[69]. Digital currencies or from a

---

[65] European Central Bank, Virtual currency schemes, October 2012, Available at https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf, Accessed on 13.04.2020.
[66] *Ibid*, p. 9.
[67] BaFin, Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer, 19.12.2013, Available at https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2014/fa_bj_1401_bitcoins.html, Accessed on 15.04.2020.
[68] *Ibid.*
[69] French Ministry of Economics, Annual report 2011, July 2012, p. 26, Available at https://www.economie.gouv.fr/files/2011_rapport_ang.pdf , Accessed on 14.04.2020.

contemporary point of view - virtual currencies - France defined as the type of money, which is not transparent[70] and mostly is used for illicit purposes[71].

As it is observable, at the very early stage of the rise of virtual currencies, different MS had different opinions, thus divided point of view can be established. Possibly, such a holistic approach can be addressed as one of the arguments why the EU failed to establish a strict and unified regulation for virtual currencies and their related service providers. If, for instance, one country within the EU recognizes and seeks to develop virtual currency utilization in the financial sector, while the other one has created a negative perception about its involvement in financial trade, the collusion arises, thus creating a complex and unsolvable set of issues, which are already hazardous in its core theory.

Nevertheless, the EU kept addressing more and more opinions regarding virtual currencies and the technological aspect behind it. In 2013, the EBA issued a warning addressed to the consumers, who are directly or indirectly involved in the transactions using virtual currencies[72]. Warning, amongst other things, raised additional concerns regarding the unregulated environment for such transactions as well as possible criminal nature in regards to ML and tax evasions[73]. This might be considered as one of the first public statements made by the supervisory authority addressing the ML concerns due to the gradual increase in popularity among persons who are operating with these financial instruments.

Years 2014 and respectively, 2015 were significant due to the incentives provided by both - EBA and ECB. EBA, in 2014, issued its opinion on virtual currencies[74], by examining key risks endangering the EU-wide financial sector as well as addressing answers to the questions related to the regulatory framework. In relation to the ML, EBA addressed two main arguments. The first one - "Criminals are able to launder proceeds of crime because they can deposit and transfer VCs anonymously."[75] And the second one - "Criminals are able to launder proceeds of crime because they can deposit and transfer VCs globally, rapidly and irrevocably."[76]. As per these concerns, it can be concluded that, after monitoring the situation after statement announced in 2013, the EBA has recognized concerns, which were established by France in already 2011. The author abstains from drawing parallels between report issued by France and information stipulated in the report[77], however clear indication of causality can be observed.

The ECB issued another report in 2015[78], which was considered as the enhancement of the previous one. Said document was introduced in 2012 in regards to the virtual currency schemes. It seeks to provide more detailed analysis of emerging trends and typologies of

[70] *Ibid*, p. 26.
[71] *Ibid.*
[72] EBA, EBA warns consumers on virtual currencies, 12 December 2013, Available at https://eba.europa.eu/eba-warns-consumers-on-virtual-currencies, Accessed on 15.04.2020.
[73] *Ibid*
[74] EBA, EBA Opinion on 'virtual currencies', 4 July 2014, Available at https://eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1, Accessed on 15.04.2020.
[75] *Ibid*, p. 32.
[76] *Ibid.*
[77] *Ibid.*
[78] Virtual currency schemes – a further analysis, February 2015, Available at https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, Accessed on 16.04.2020.

virtual currencies. On the contrary side of the previously issued report, this, as well as the EBA's, seeks to emphasize the side, which consists of entitled risks[79] due to the fact that decentralized virtual currencies such as Bitcoin has become more and more popular and the mining of it have only increased since its establishment[80].

Eventually, after the key EU level watchdogs have shared their opinions and guidelines in regards to the virtual currencies, the author of this work would not like to go into more detail due to the fact that, for the purposes of this section, it was necessary to comprehend primordial incentives rather than currently existing ones. Afterwards, this paper will examine regulatory requirements governing virtual currency service providers in Latvia and elsewhere in the EU.

As for the concluding remarks, it is observable that the EU authorities started to identify issues and cornerstones right after this method of payment achieved its primordial popularity boost. After it has been operating in the market for some time, authorities began monitoring activities on a global and local level, by supervising each MS's capabilities to deal with arising form of financial instrument. As from the economics perspective - since it was never recognized as conceivable money, it failed to fulfil major roles[81], which characterized it:

1) Limited ability to store a reliable value due to the high price volatility[82];

2) Acceptance network restricts its usage as a medium of exchange[83];

3) Represents the value against the exchange rate not against the value of involved good/service.[84]

1.3.2.2. The national context

As it was mentioned elsewhere in the thesis, the year 2014 and 2015 turned out to be a remarkable reference point for virtual currencies to start their rise in the global market. In parallel to the ongoing situation in the EU, Latvian national airline carrier "AirBaltic" announced that Bitcoin will be accepted as an alternative payment method[85], thus becoming the first such service provider in the EU offering particular alternatives[86]. On the contrary, *Latvijas Banka* (in English - the Central Bank of Latvia) collectively with the FCMC issued a joint warning whereas it was stated that Bitcoin should not be perceived as a payment method due to the lack of regulation and characteristics, which defines money as people tend to

[79] Ibid, p. 32, Conclusion.
[80] Blockchain.com, Total Circulating Bitcoin, Available at https://www.blockchain.com/charts/total-bitcoins, Accessed on 16.04.2020.
[81] Dong He, Karl Habermeier, Ross Leckow, Vikram Haksar, Yasmin Almeida, Mikari Kashima, Nadim Kyriakos-Saad, Hiroko Oura, Tahsin Saadi Sedik, Natalia Stetsenko, and Concepcion Verdugo-Yepes, Virtual Currencies and Beyond: Initial Considerations, January 2016, p. 17, Available at https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf, Accessed on 17.04.2020.
[82] *Ibid*, page 17.
[83] *Ibid.*
[84] *Ibid.*
[85] AirBaltic, AirBaltic - World's First Airline To Accept Bitcoin, Riga, 22.07.2014, Available at https://www.airbaltic.com/airbaltic-worlds-first-airline-to-accept-bitcoin, Accessed on 18.04.2020.
[86] Thompson Reuters, Latvia, Cryptocurrencies by country, 25 Oct 2017, Available at https://blogs.thomsonreuters.com/answerson/world-cryptocurrencies-country/, Accessed on 19.04.2020.

comprehend it[87]. This previously specified lack of regulation have risen deep concerns whether such payment method should be tolerated at all. On the hand, cross border juggernaut watchdogs have stated and publicly announced that virtual currencies underline several risks, which must be tolerated as a potential threat for the EU-wide financial sector, while on the other hand, MS are keen to implement this alternative financial instrument in their integrated financial sectors.

This, however, drives a conclusion, that MS are keen to extend their monetary taxonomy by introducing new and attractive ways of conducting transactions/deals[88]. By extending specified sphere, peer-to-peer and decentralized nature seeks to attract more and more customers from abroad, thus guaranteeing greater national-level cash flow, whereas potential risks are treated to be almost non-existent and irrelevant.

Latvian State Revenue Service (hereinafter referred to as the "SRS") in 2017 issued a comment clarifying taxation aspects which surrounds virtual currency aspect[89]. It has been stated that virtual currencies should be considered as commodities and therefore, according to the Law on Personal Income Tax, taxation matters should be calculated in the amount of 23%[9091], whilst in 2015 judgment of the Court in case C-264/14 ruled that Bitcoin in particular can be considered having the nature of the currency[92] (thus can be recognized as a means of payment), therefore transactions concluded by using this cryptocurrency should not be regarded as the subject for VAT taxation[93].

Eventually, contemporary comprehension from the perspective of Law of Personal Income Tax states that virtual currencies are recognized as capital assets[94], whilst the Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing subjects virtual currency service providers[95] to be compliant with this law in order to offer services to the general public. As per the regulation[96], virtual currency service providers are supervised by the SRS.

---

[87] Žanete Hāka, Latvijas Banka un FKTK: Bitcoin nav ne valūta, ne maksāšanas līdzeklis 23.07.2014, Available at https://www.db.lv/zinas/latvijas-banka-un-fktk-bitcoin-nav-ne-valuta-ne-maksasanas-lidzeklis-417958, Accessed on 19.04.2020.

[88] Fordham Law School, Virtual Currencies and the Challenges to Compliance Wednesday, Fordham/Accenture Compliance Series, 13.06.2018 p. 59, Available at fordham.edu/download/downloads/id/10965/Accenture_Compliance_Virtual_Course_Materials.pdf

[89] Valsts ieņēmumu dienests, Par darījumiem ar kriptovalūtu un nodokļiem, 08.06.2017, Available at https://lvportals.lv/e-konsultacijas/11918-par-darijumiem-ar-kriptovalutu-un-nodokliem-2017, Accessed on 19.04.2020.

[90] *Ibid.*

[91] Law on Personal Income Tax (Likums "Par iedzīvotāju ienākuma nodokli"), Latvijas Vēstnesis, 32, 01.06.1993. Available at https://likumi.lv/ta/id/56880, Accessed on 20.04.2020.

[92] Judgment of the Court (Fifth Chamber) of 22 October 2015, Skatteverket v David Hedqvist, Request for a preliminary ruling from the Högsta förvaltningsdomstolen, Case C-264/14. Para. 28-31, Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0264, Accessed on 20.04.2020.

[93] *Ibid*, para 57.

[94] *Supra* note 90, Section 11^9.

[95] Article 1, Para. 2^2, Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing (Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma un proliferācijas finansēšanas novēršanas likums), Available at https://likumi.lv/ta/id/178987, Accessed on 20.04.2020.

[96] *Ibid*, Article 3, Para. 1^{11}.

2. VIRTUAL CURRENCIES IN THE EU AND LATVIAN AML REGULATORY FRAMEWORK

The previous chapter provided a comprehensive idea of what essentially AML is, what are the key components of it and what regulatory steps have been taken in order to regulate operability of virtual currencies on the EU level. As per analysis conducted beforehand, the author emphasizes incentives taken by the supervisory watchdogs, which, essentially, could be classified as clarification seeking and opinion providing activities for the purposes of acknowledging existence of said financial instruments/currencies in the EU's financial sector. This, as a result, corresponded to introducing virtual currencies[97] as defined term in the AML 5th directive, which, eventually, by consisting of legally binding nature, created an obligation to MSs to transpose its amended requirements into national legislation. These amendments, nevertheless, established that virtual currency service providers must be recognized as the subjects of the respective AML law[98].

2.1. Analysis and interpretation of the AML 5th directive - provisions governing virtual currencies and virtual currency service providers on the EU level

The major amendments regarding the virtual currencies, as stated previously, touches upon the requirements to ensure that virtual currency service providers should now be considered as the subjects to the 5th AML directive. Eventually, the directive does not specifically define virtual currency service providers as such. In other words, it has been stated as "providers engaged in exchange services between virtual currencies and fiat currencies"[99].

Extended scope introduces the term "fiat currencies". As per the clarification provided by the ECB, the fiat currency is "value designated as legal tender, typically in the form of notes or coins"[100] (*e.g.* EUR, USD, GPB).

By analysing the whole term collectively, a key "finding" can be already observed. From the first glance, it is not clear, whether subjects to the AML law should be persons, who are offering services to the third party (for instance - legal entity offers its services to the customer in exchange receiving fiat currency), or whether subjects to the AML law should also be persons, which are conducting an entity-to-entity transaction (for instance - legal entity conducts a transaction with other legal entity, whereas both have agreed to trade Bitcoin to the US dollar, without involving a conversion element[101], for instance)[102].

---

[97] *Supra* note 49.
[98] *Ibid*, Para. 29.
[99] *Ibid*, Para. 1[cg].
[100] EBA, Report with advice for the European Commission, 09.01.2019, p. 12, Available at https://eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf?retry=1 , Accessed on 22.04.2020.
[101] Conversion element - must be understood as a set of actions whereas one party exchanges currency to the other currency by considering actual and real-time exchange rate, thus determining value for an exchangeable.
[102] Nejc Novak, EU Introduces Crypto Anti-Money Laundering Regulation, 02.01.2018, Available at https://medium.com/@nejcnovaklaw/eu-introduces-crypto-anti-money-laundering-regulation-d6ab0ddedd3, Accessed 22.04.2020.

As per understanding the directive itself, the proposed scope is attributable to the situations whereas services related to the virtual currencies are offered in a format of business-to-customer relationship, not, as it was assumed for the explanatory purposes, in the format of a business-to-business relationship. In addition, the FATF has taken an incentive and defined that virtual currency service providers must be recognized as persons, which "[...] conducts activities which fall within the FATF definition of a financial institution[103] [...]. This includes convertible virtual currency exchangers where convertible VC activities intersect with the regulated fiat currency financial system"[104]. Therefore, by considering FATF's involvement in clarifying issues related to the virtual currencies, adopted definition underlines the scope, whereas the virtual currency service providers are engaging in business-to-customer type of relationship.

Furthermore, after the directive's scope has been clarified, it is necessary to comprehend minimum requirements set by the said document since the regulator has imposed an obligation to MS to implement the said provision.

Minimum requirements, in general, must be observed in respective jurisdiction legislation, since some nuances of the directive itself can be interpreted differently, by considering attributable unique risk factors, which particular geographic region faces. This, in particular, will be analyzed further in the thesis, whereas Latvian regulatory requirements will be considered to assess compliance norms for virtual currency service providers.

Prior to providing an explanation to the following, a synergy between the AML 4th and the AML 5th directive must be understood, therefore an overall comprehension will be established.

As it is observable, the AML 5th directive is an amending part to the previous AML 4th directive, which was passed as an enhanced version of the 3rd AML directive. Eventually, the 4th AML directive emphasized several risk based approach[105] requirements, which were designated for the MSs to implement them in their national legal systems. This risk based approach means low-level assessment and comprehension of residual and inherent risks that particular country is facing. Moreover, reinforced KYC/CDD requirements for the subjects of the law were introduced in order to extend the existing scope of examining relationship between the subject of the law and the customer.

Furthermore, since the AML 4th directive still is in force, its requirements are still directly applicable to the MS, therefore amendments made by the 5th directive supplements the 4th directive and extends the scope of it. Eventually this means that existing general directive (AML 4th directive) has currently been reinforced, therefore, its requirements are now also directly applicable to the subjects of the law, which were introduced by the 5th directive (in this case - virtual currency service providers).

[103] FATF, Financial Institutions, FATF Glossaries, Available at https://www.fatf-gafi.org/glossary/d-i/, Accessed on 23.04.2020.

[104] FATF, Guidance For A Risk-Based Approach, Virtual Currencies, p. 7, Available at https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf , Accessed on 24.04.2020.

[105] Deloitte, The Fourth EU Anti Money Laundering Directive, 2015, Available at https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/FinancialServices/investmentmanagement/ie_2015_The_Fourth_EU_Anti_Money_Laundering_Directive_Deloitte_Ireland.pdf, Accessed on 24.04.2020.

Nevertheless, since virtual currency exchange service providers have been classified as the subjects of the law, AML 4th directive requirements are therefore directly applicable, however, the issue already arises - the AML 4th directive came in force in 2015, whilst the AML 5th directive came in force in 2018, meaning that requirements established in 2015 were designed for subjects of the law, which were identified for the purposes of the 4th AML directive.

This particular nuance, eventually, means, that theoretically, due to the reason, that virtual currencies as such were recognized as defined term only in 2018, and understanding the fact, that the technology behind virtual currencies is rather complicated and not yet regulated by the legislative authority, threats arising from this subject cannot be theoretically comprehended by the 4th AML directive scope. Indeed, it is possible to identify similarities, typologies with other types of financial services and currency exchange service providers, however, *ex ante* methodology cannot be adopted on general regulatory-matters basis.

By establishing a fictitious scenario, let's suppose that all the regulatory requirements are directly applicable to the virtual currency service providers. As an example, let's consider suspicious transaction reporting (hereinafter referred to as the "SRS", in the 4th AML directive referred to as the unusual or suspicious transactions/activity[106]) as a requirement, which must be addressed whenever a subject of the law identifies that there are suspicious/unusual nature of the transaction or activity[107]. Having said that, suspicious activity can be identified by assessing different characteristics against executed transactions/observed nature either provided by the national law, international guidelines or internal governance. For the sake of the argument, let's suppose that the virtual currencies service provider has implemented all the risk identification related characteristics into its internal policies and procedures. Among the other things, the first issue arises - to what extent and how greatly the subject is required to investigate nature of the transaction, for instance? For example, currency exchange has been conducted from EUR to the Bitcoin (an abbreviation of "BTC" will be used further in the text, if it is connected to the Bitcoin as means of payment). Basically, the company X, which provides currency exchange services is required to buy BTC, whilst in exchange giving EUR to the third party. As per understanding that blockchain offers pseudonymity[108], the deal itself will be rather transparent than opaque, however if other currency would be involved with more stricter anonymity requirements, the situation would be that nor nature nor transaction's reasoning could be classified as suspicious only by the fact that there are no particular characteristics set by the law/guidelines. This, eventually, could lead to opposite false-positive cases, where due to the lack of regulation, all the transactions and behaviors could not be noticed since regulatory framework was not originally designated to regulate such types of transactions/behavior. Of course, such requirements as identification or verification of the customer can be satisfied, but regardless of that, the AML does not stops after understanding who or what is particular institution's customer.

[106] Article 14^4 and 15^5, Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.
[107] Ibid, 15^5 and 18^2.
[108] Jamie Moy, Forget Bitcoin, It's All About The Blockchain, Forbes, 22.02.2018, Available at https://www.forbes.com/sites/jamiemoy/2018/02/22/forget-bitcoin-its-all-about-the-blockchain/#2d12f04b5f6b, Accessed on 25.04.2020.

As it was mentioned beforehand, the scope of the AML 5th directive covers only those virtual currency service providers, who are offering currency exchange as a service, *i.e.* person holds certain amount of BTCs and is willing to trade them against the fiat currency of EUR, for instance.

As per having this in mind, primordially it is not clear what risks except ensuring the counterparty with the fiat currency can else arise due to this line of service. Indeed, this type of exchange underlines certain sanctions risk exposure as well possible ML risk exposure due to the opaqueness, however, it is not clear how far does the virtual currency service provider is required to regulate itself.

Let's suppose, that by having implemented all the regulatory requirements in institutions procedures, the institution, accordingly has obtained the said BTC. For the purposes of this example, the author seeks to assume that all the minimum requirements set by the law are treated respectively and accordingly. Moreover, after the BTC has been obtained, the question further arises - since the fiat currency has been exchanged to the virtual currency, most likely the said institution will make financial speculations with it *i.e.* trade it in the exchange platform. Taking this into account - is the institution required to somehow monitor their activities in respect to the AML provisions? As far as it has been defined, stock exchange must validate and identify whether their customer funds (institution in our example) are legitimate and with understandable nature, but there's nothing stated in the directive that the said virtual currency service providers must monitor and supervise their own further activities.

Hence, since the scope was extended by introducing the term of virtual currency service providers, also supervisory activities have been reinforced by setting as a requirement for MS to ensure that "providers of exchange services between virtual currencies and fiat currencies, and custodian wallet providers, are registered [...]"[109]. Understanding hereby written, the provision emphasizes the word "registered" not "licensed", for instance, therefore, by applying common approach, the requirement does not create an obligation for MS to have additional requirements for issuing a license whereas it would be in the case with the credit institution, for instance. Moreover, the respective AML authority in the jurisdiction is required only to maintain a register where particular subjects are listed for a general consumer availability, thus avoiding any specific intervention in its credibility or business practice[110], which would be in a case with the requirement to issue specifically tailored licenses.

2.2. AML minimum regulatory requirements in Latvian legal system in regards to the virtual currency service providers

Beforehand, the author of this thesis emphasized key elements, which describes AML as a risk-based tool used in order to mitigate and combat ML possessed threats as well as clarified and analyzed the scope of the AML 5th directive in relation to the virtual currency service providers. The EU-wide context provided a primordial understanding and comprehension of

[109] *Supra* note 103, Para. 29.

[110] ECB, Lecture by Tommaso Padoa-SchioppaMember of the Executive Board of the European Central Bank, Washington D.C., 24.09.1999,Available at https://www.ecb.europa.eu/press/key/date/1999/html/sp990924_1.en.html , Accessed on 25.04.2020.

how the virtual currencies and their service providers are perceived, therefore giving an indication of what might be expected in the national regulatory framework.

The governing and general AML law in Latvia is the Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing (hereinafter referred to as the "Latvian AML law"). It provides general requirements and scope of what are the primordial compliance norms for each of the subject of the law. According to the purpose of the law "[...] to prevent money laundering and terrorism and proliferation financing."[111], it can be established that the specific legal act, regardless of other supplementary provisions, serves the sole purpose of regulating the market in a generic manner.

2.2.1. Supervisory authority

Prior perceiving minimum requirements established in the law, which regulates virtual currency service providers from the AML perspective, it is necessary to examine the competent authority, which is responsible for supervising the business activity of the said subject.

Article 45, paragraph 2, sub-paragraph 6e[112] of the Latvian AML law stipulates that the sole supervisory authority of the virtual currency exchange service providers is the State Revenue Service (hereinafter referred to as the "SRS"). Unlike in case with the credit institutions and the FCMC as the supervisory authority, for instance, the SRS is directly responsible for regulating the market and its participant's activities in regards to the AML provisions. As it was stipulated in the 5th AML directive, the competent authority is also responsible for maintaining the subject of the law register, hence corresponding regulatory requirement can be found in the Article 46 of the Latvian AML law[113].

At first glance, the rationale behind appointing the SRS as the competent supervisory authority remains unclear since foreign currency exchange service providers are directly supervised by the *Latvijas Banka*[114]. The nature behind exchanging fiat currency to other foreign fiat currency is equivalent to nature whereas virtual currency is exchanged to other virtual currency, for instance. This, however, raises concerns due to the fact that currency exchange service sector in general in the EU MSs has been exposed to the ML threats. The concern was already raised on the EU level in 2010, where the FATF identified key issues concerning customer risk and lack of legislative powers to regulate this sphere of financial services. In general - whenever the currency exchange used to occur, small payment tranches were involved, thus hindering the possibility to establish comprehension of the source of funds[115].

Nevertheless, the same difficulty was established by *Latvijas Banka* in the annual risk assessment report. It was stated, that due to the fact that these transactions have immediate exchange nature, respective service providers lack resources and general capacity to be

[111] *Supra* note 95, Article 2.
[112] *Ibid*, Article 45.
[113] *Ibid*, Article 46.
[114] *Ibid*, Article 45, Para. 6.
[115] FATF, Money Laundering through Money Remittance and Currency Exchange Providers, 2018, p. 21, Available at https://rm.coe.int/fatf-report-money-laundering-through-money-remittance-and-currency-exc/16807150ad , Accessed on 27.04.2020.

completely compliant with the requirements set by the regulator, thus failing to ensure fully comprehensive due diligence measures *i.e.* understanding the source of funds or assessing the trustworthiness of the received information from the customer[116]. These deficiencies, nevertheless, thrives from rapid cash involvement, which, eventually, may lead to opaqueness and anonymity issues.

As it was discussed previously, in Latvia there is more than one supervisory authority. Other such as the Consumer Rights Protection Centre, SRS, FCMC, they all have their own scope of supervisory obligations, thus emphasizing the variety of provided financial services in the territory. Having said that, the obvious conclusion can be derived that due to the fact that each of the supervisory institution has their own scope of competence, their risk tolerance might be different, and therefore further application of the requirements towards the subjects of the law may not consist of the same methodology. Basically, if, for instance, the SRS is responsible for supervising cash collection service providers[117], its overall risk assessment and application of compatible regulatory requirements may focus on different inherited and residual risk indicators than it would be in case with the FCMC, for instance.

Previously defined discrepancy was also identified by the Moneyval examination. The institution in its report provided an observation, which stipulated that due to the large number of supervisory authorities in the state, misleading and even inconsistent interpretation of the law by each of the supervisory authority led to the general compliance gaps[118], which eventually were considered as crippling in regards to the further execution and application process. Additionally, due to the same issue, widely differentiated knowledge level in this regard was also noted as one of the emerging issues[119], more particularly - when the actual sectorial risk was considered to be high, supervisory authority treated it as low or medium risk sector[120].

On the one hand, variety of supervisory authorities seems to be considered as a failure in regards to the effective supervision, nevertheless - if the respective authority is responsible for a certain number of subjects of the law, it is not overwhelmed with the monitoring and supervision duties, which could arise in the case where only one institution has a sole competence to regulate the market. Therefore such methodological approach has their own pluses and minuses.

Eventually, at the beginning of this section, the author of this thesis raised the concern about the competences, which the SRS have in regards to the supervision of AML provisions. Having understood the overall risk comprehension in the sector of foreign currency exchange, it must be kept in mind that virtual currencies are not treated as a legal means of payment[121].

---

[116] Central bank of Latvia, Ārvalstu valūtu skaidrās naudas pirkšanas un pārdošanas sektora noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas risku novērtējums, 2019, p. 3-4, Available at https://www.bank.lv/images/stories/pielikumi/valutasmaina/Sektorialais-risku-novertejums-Latvijas-Banka-02042019.pdf , Accessed on 27.04.2020.

[117] *Supra* note 95, Article 45 para. 6 d).

[118] MONEYVAL, Anti-money laundering and counter-terrorist financing measures Latvia Fifth Round Mutual Evaluation Report, 2018, p. 104, Available at https://rm.coe.int/moneyval-2018-8-5th-round-mer-latvia/16808ce61b, Accessed on 28.04.2020.

[119] *Ibid*, p. 105.

[120] *Ibid.*

[121] Article 3^3, Law on the Procedure for Introduction of Euro (Euro ieviešanas kārtības likums), Latvijas Vēstnesis, 33, 15.02.2013, Available at https://likumi.lv/ta/id/254741, Accessed on 28.04.2020.

This, eventually means, that although the rationale behind the executed action is quite similar in case with fiat currencies, the involved instruments triggers tax law related issues. Therefore instead of having a fiat-to-foreign currency transaction, rather barter has been established and virtual currency service providers are just maintaining their economic activity without involving the actual element of exchange.

2.2.2. Scope of the law and key defining terms

Having comprehended the core fundamental of the Latvian AML law and clarifying aspects, which surrounds supervisory authority and keeping in mind that the sole purpose of this thesis is to analyze virtual currency regulatory framework, the author of this work ought to begin with by providing two definitions, which stems from the Latvian AML law.

> **virtual currency** - a digital representation of the value which can be transferred, stored or traded digitally and operate as a means of exchange, but has not been recognised as a legal means of payment, cannot be recognised as a banknote and coin, non-cash money and electronic money, and is not a monetary value accrued in the payment instrument which is used in the cases referred to in Section 3, Clauses 10 and 11 of the Law on the Payment Services and Electronic Money[122]

And

> **virtual currency service provider** - the person providing virtual currency services, including the provider of services of exchange of the virtual currency issued by other persons, which provides the users with the possibility to exchange the virtual currency for another virtual currency by receiving commission for it, or offer to purchase and redeem the virtual currency through a recognised legal means of payment[123]

The definition of virtual currencies is quite similar to the one, which has been defined by the AML 5th directive. Therefore the common denominator of "non-fiat currency" and "digital representation" establishes that Latvian legislative body and overall risk tolerance is in line[124] with the perception amongst the EU legislators. Moreover, the scope of the virtual currency service providers has been reinforced by specifically defining what kind of services are considered to be supervised in regards to the Latvian AML law. These services, however, are:

1) Purchase of the virtual currency by paying using the euro currency[125];
2) Sale of the virtual currency by receiving euro currency[126];
3) Virtual currency exchange to other virtual currency[127];
4) Persons operating virtual currency ATMs[128].

---

[122] Ibid, Article 1^{22}.
[123] Ibid, Article 1^{23}.
[124] European Commission, Complexity of EU law in the domestic implementing process, Brussels, 03.07.2014, Available at https://ec.europa.eu/dgs/legal_service/seminars/20140703_baratta_speech.pdf , Accessed on 29.04.2020.
[125] State Revenue Service, Virtuālās valūtas maiņas pakalpojumu sniedzēji, Available at https://www.vid.gov.lv/sites/default/files/2_8_virtualas_valutas_mainas_pakalpojumu_sniedzeji.pdf, Accessed on, 30.04.2020.
[126] *Ibid.*
[127] *Ibid.*
[128] *Ibid.*

As it was established previously, listed services indeed consist of exchange nature proceedings, *i.e*. if the person X is seeking to sell BTC, he/she/it will not be considered as the subject of the law, if the agreed value of the tradable currency will be determined regardless of the existing exchange rate between involved financial instruments.

2.2.3. Minimum requirements set in the Latvian AML law

The very first requirement set by the Latvian AML law was mentioned previously, whereas supervisory authority's compatibility was discussed. As per Article 45, paragraph 3, virtual currency service providers are required to register their economic activity and after 10 business days inform the SRS about expected type of its activity[129]. This, eventually, must be done in accordance with the Article 10, which requires subject of the law to appoint responsible compliance employee(-s) for the fulfilment of regulatory provisions[130] and senior-level executive, whose competences would allow him/her to make final and decisive decisions in regards to the detected internal issues in relation to the AML[131]. This obligation involves being directly responsible for ensuring compliance with the regulatory requirements[132].

Particular taxonomy can be observed in the report issued by the Basel Committee on Banking Supervision (hereinafter referred to as the "Basel")[133]. It seeks to clarify that senior management executives are the core delivery team for ensuring compliance with the institution's risk exposures, appetite[134] due to the fact that they supervise institutions tone of the top, which eventually, involves comprehending regulatory requirements in respective spheres of work. Sound governance in this case means fully compliant AML procedures, policies and mechanisms.

Whenever the registration (not licensing) process has been conducted, proceeding requirement demands subject of the law to perform a risk assessment and afterwards establish internal control system, by considering national/internal assessment results and other risk increasing factors.

In regards to it, the Latvian AML law stipulates that whenever the subject of the law (virtual currency service provider) performs a risk assessment or creates an internal control system, it must take into account risk identified by the European Commission[135] (supranational risk assessment), national risk assessment[136] and other, which are relevant to the respective economic activity[137].

Having said that, the practical approach works in a way that the subject of the law in this case takes into account supranational risk assessment and national risk assessment however particular risks inherent to the virtual currency service providers are addressed in the report issued by the FIU and SRS. Among the other things, the FIU has established the

[129] Supra note 95, Article 45, Paragraph 3.
[130] *Ibid*, Article 10 (1).
[131] *Ibid.*
[132] *Ibid.*
[133] Basel Committee on Banking Supervision, Principles for enhancing corporate governance October 2010, Available at https://www.bis.org/publ/bcbs176.pdf, Accessed on 30.04.2020.
[134] *Ibid*, p. 24.
[135] Supra note 95, Article 6, Para.16 1^1.
[136] *Ibid.*
[137] *Ibid.*

concern that companies, which are offering virtual currency related services, are considered as high risk companies[138], therefore further incentives to establish business relations with banks or other financial institutions, and might rise additional difficulties. Nevertheless, due to the fact, that each financial institution has an authority to establish its own risk appetite and tolerance (meaning, it decides what level of risk thriving from the customer is acceptable in order to pursue with business relations), the game of luck in relation to virtual currency service providers and further cooperation can occur. This means that whenever there will be institutions, which are ready to tolerate high risk customers and business relation, virtual currency service providers can pursue with operating their business.

Regardless of previously stated, the author of this thesis is willing to elaborate on risks identified by the FIU and SRS due to the fact that specific risk addressing requires certain further actions.

As per the FIU has established, in regards to the virtual currencies, major risks, mainly, derives from anonymity, which was addressed by the EBA in 2014[139]. The SRS, as being the supervisory authority, also has clarified, that key risks, which must be taken into account prior establishing internal controls and scoring systems are anonymity[140], transaction pace[141], opaqueness[142], untraceable money flow[143] and cross-border transaction concerns[144]. These five identified risks must be respected in respective scoring systems and internal controls. Comprehending the fact, that some of the risk indicators are rather abstract, the challenge to ensure utmost compliance will arise thus leading to possible gaps, loopholes and false-positive result emerging[145]. To avoid such situations, by logic there should be available regulatory guidance provisions in order to assist subjects of the law with their incentives to be compliant with the law, however giving the fact, that these identified risks are rather abstract, it is impossible to establish unified guidance provisions[146], *ergo* leaving a wide room for interpretation.

Furthermore - after the internal control and scoring system requirements have been set straight, due diligence and reporting requirements are the subsequent binding provisions, which must be respected by the virtual currency service providers.

Article 11[147] provides situations whereas virtual currency service providers are required to conduct the CDD. Almost everything, what is stipulated there, must be respected, therefore regulatory burden becomes quite comprehensive. These requirements, *inter alia*,

---

[138] Noziedzīgi iegūtu līdzekļu legalizācijas novēršanas dienests, Virtuālās Valūtas Noziedzīgi Iegūtu Līdzekļu Legalizācijas Un Terorisma Finansēšanas Riski, Available at https://www.fid.gov.lv/images/Downloads/useful/Riska_nov_virt_valutas_LV.pdf , Accessed on 01.05.2020.
[139] *Ibid*, p.7-9.
[140] *Supra* note 125.
[141] *Ibid.*
[142] *Ibid.*
[143] *Ibid.*
[144] *Ibid.*
[145] Fedor Poskriarov, Maria Chiriaeva, Christope Cavin, Managing AML compliance risks, Blockchain and Cryptocurrency Regulation 2020, Cryptocurrency compliance and risks: A European, KYC/AML Perspective, Available at https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/11-cryptocurrency-compliance-and-risks-a-european-kyc-aml-perspective , Accessed 01.05.2020.
[146] *Ibid.*
[147] *Supra* note 95, Article 11.

provides basis for reporting to the FIU[148] in case if lack of information or suspicious activity has been detected[149]. As per understanding the law, these requirements were designated for the subjects, which were introduced by the third and fourth AML directive, therefore their applicability might rise challenges in regards to the virtual currency service providers. For instance - understanding the fact, that provided exchange services consists of immediate nature, there might be situations where it could be merely impossible to detect suspicious transactions at all, thus leading to unreported potential money laundering and terrorist financing cases[150].

Article 11^1, 12 and 13 provides basis for KYC requirements. These, nevertheless, are intended in order to identify potential customer prior establishing business relations (also, these requirements must be respected during existing business relation[151]). Due to the fact, that transaction monitoring in this regard might rise challenges, KYC framework should be as robust as possible, since primordial compliance thrives from properly identifying the potential service user/customer. Having said that, there are no additional and tailored requirements for virtual currency service providers to consider prior identifying customer, however, since this type of service underlines new risks, the classic identification approach might not be sufficient.

One of the requirements, which could reinforce the whole identification process, touches upon the IP addresses[152]. *I.e.* whenever the virtual currency service provider has an opportunity to establish new business relations, potential IP address, which is perceived to be used, should be obtained. In practice this could assist in identifying red flags stemming from customer's activities, ergo whenever the exchange transaction occurs from different IP address, automatically generated alert indicates that there is a discrepancy, which requires further investigation. The same methodology could be used in a way, that the service provider obtains computer machine-ID and ensures that it gets validated whenever the person is logging into its account or making the transaction.

Indeed, it is possible to already establish certain opposing arguments for why this could lead to regulatory burden, such as - whenever the person changes the location, its IP address will also be changed, persons tend to acquire new computers, *etc*., however, comprehending the fact that virtual currencies already possess high risk to the financial sector and perceiving ,that part of people are conducting/executing transactions while being physically at the same spot, such step could at least, at minimum, reinforce the identification and monitoring scope, thus increasing the possibility to avoid money mulling[153] or any unconfirmed third person involvement. This, eventually, also could alert occasions, whenever there might be a high difference between registered geography and actually used, while also

[148] *Ibid.*
[149] *Ibid.*
[150] Ross Leckow, Virtual currencies: the regulatory challenges, p. 137, Available at https://ccl.yale.edu/sites/default/files/files/Leckow_Ross_Virtual%20currencies%20-%20the%20regulatory%20challenges.pdf , Accessed on 02.05.2020.
[151] *Supra* note 95.
[152] UNODC, Virtual Currencies, p. 95, Available at https://www.imolin.org/pdf/UNODC_VirtualCurrencies_final_EN_Print.pdf , Accessed on 02.05.2020.
[153] U.S. Department of Justice Federal Bureau of Investigation Money laundering, Forfeiture and Bank Fraud Unit, What Is a Money Mule, Money Mule Awareness, Available at https://www.fbi.gov/file-repository/money-mule-awareness-booklet.pdf , Accessed on 02.05.2020.

taking into account time pace between last executed transaction and current. Nevertheless, such solution should be tailored taking into account potential compliance costs and potential customer outreach, assuming that there is an employee who contacts the customer immediately after the alert has been detected.

Aforementioned is one of many example of what particular identifications steps could be used in order to reinforce the KYC protocol. At some point, this could ease the compliance burden in a way that more possible SAR reports to the FIU would be made and also "bad customer" portfolio would clear out naturally. Eventually, as per the Latvian AML law, all obtained identification related information must be verified against respective independent and reliable sources[154].

By expanding on the identification requirement, the Latvian AML law as an inevitable requirement, has subjected the transaction monitoring requirement on frequent and continuous basis[155]. Hereby, as it was stated elsewhere in the thesis, the core nature of exchange services relies on immediate transaction pace, which essentially impacts utmost compliance. Notwithstanding the scope of the transaction monitoring, it goes hand in hand with the enhanced due diligence (hereinafter referred to as the "EDD") and simplified due diligence[156] (hereinafter referred to as the "SDD") requirements, since it involves transaction and customer in-depth analysis[157]. However in this case, due to the fact that virtual currency business is considered to have a high risk economic activity, EDD should be performed on more frequent basis than SSD, thus ensuring utmost compliance and avoiding any potential regulatory discrepancies.

By having lack of tailored regulatory guidelines/requirements in this regard, the monitoring itself should be established on already existing foundations or guidelines, which are applicable to other alike subjects of the law - foreign currency exchange services or at some point exchange as such. The rationale behind such approach, although, has not been stipulated by legislators, could stem from similarities in economic activity and provided services, therefore in order to perform sufficient transaction monitoring, virtual currency service providers could adopt transaction scenarios identified by international watchdogs, *Latvijas Banka* and the SRS, for instance. Mentioned transaction scenarios works in a way that, for instance, the law addresses or the supervisory authority has identified specific risks, which are quite substantive and points out possible fraudulent activity options. Eventually, the institution, which is considered as the subject of the law, is required to implement these scenarios in algorithmic way, considering their magnitude, thresholds and technical scope. As per ACAMS has clarified, proper scenario implementation ensures risk focused transaction detection[158], internal compliance gap detection[159] and automatic alert generation if thresholds

[154] *Supra* note 95, Article 11^{1}.
[155] *Ibid*, Article 20^{12}.
[156] *Ibid*, Article 26.
[157] *Ibid*, Article 22.
[158] Luis Canelon, Carl Hatfield, Chetan Shah, Anti-money laundering transaction monitoring system implementation considerations, 31.05.2013, https://www.acamstoday.org/anti-money-laundering-transaction-monitoring-system-implementation-considerations/, Accessed on 02.05.2020.
[159] *Ibid.*

are set[160]. These three main advantages seeks to ease compliance burden and reinforce internal control efficiency.

Hence, considering Latvian approach, the counter comparison must be addressed by introducing industry best practice, which in this case stems from the US. Due to the fact, that the US financial sector is attractive for people seeking money laundering activities[161], their adopted regulatory approach will serve the purpose for developing an argument.

The report issued by the audit company KPMG describes an approach introduced by the US authorities - alongside the transaction monitoring requirements[162], there are requirements stipulating the transaction filtering. This filtering, however, in other words, serves the key purpose of detecting and indicating the transactions, which are related to the OFAC (the Office of Foreign Asset Control) announced regimes or sanctions[163]. In practice that means that virtual currency service providers are required to adopt OFAC risk assessment directly, thus ensuring compliance with it.[164] Ergo it means, that whatever inherent risks OFAC has identified, they must be implemented in the subject's internal control system, thus - extended transaction monitoring/filtering policy.

Eventually such diversification robust the whole monitoring process due to the fact that unified approach in terms of detecting sanction or ML violations/schemes has been adopted by all industry subjects. Indeed, Latvian regulatory framework also requires to establish a sanction monitoring system, however the key difference is that there is no obligation, which requires a particular subject of the law directly take into account national sanction risk assessment[165] or related document. Hence, it must be based on it, however it is not directly binding or applicable.

Furthermore, as it was discussed previously, the subject of the law is responsible for reporting on suspicious transactions/activity[166], if one has been detected or observed. Therefore, in case if the virtual currency service provider has obtained information, which rises legitimate concerns (regardless of the transaction status), immediate actions are required. Additionally, immediate reporting requirements must be respected in case of submission of threshold declaration[167]. Respective provisions sets two detailed scenarios when the submission is necessary, *i.e.* - when the customer executes cash transaction, which is equivalent to the amount of 7000 EUR[168], and when the customer receives or executes cross-border transaction (not necessarily cash transaction) equivalent to the amount of 500 000

[160] *Ibid.*
[161] Executive Summary, National Money Laundering Risk Assessment, 2018, Available at https://home.treasury.gov/system/files/136/2018NMLRA_12-18.pdf , Accessed on 02.05.2020.
[162] KPMG, Cross border cryptocurrency compliance, p. 9, Available at https://advisory.kpmg.us/content/dam/advisory/en/pdfs/cross-border-cyryptocurrency-compliance.pdf , Accessed on 05.05.2020.
[163] ACAMS, Understanding the new DFS Part 504 Regulations and the Associated AML Program testing Challenges, p. 16, Available at http://files.acams.org/pdfs/2017/Understanding_the_New_DFS_Part_504_Regulations_C.Recor.pdf , Accessed on 05.05.2020.
[164] *Ibid.*
[165] Article 8, Sanction Risk handling rules (Sankciju riska pārvaldīšanas normatīvie noteikumi), Available at https://m.likumi.lv/doc.php?id=304787 , Accessed on 05.05.2020.
[166] *Supra* note 95, Section 4.
[167] Ministru kabineta 2019. gada 27. augusta noteikumi Nr. 407 "Noteikumi par sliekšņa deklarācijas iesniegšanas kārtību un saturu". Latvijas Vēstnesis, 182, 06.09.2019, Available at https://likumi.lv/ta/id/309171, Accessed on 05.05.2020.
[168] *Ibid,* Article 5.1.1.

EUR[169]. These thresholds, however, are introduced in order to supplement existing internal controls[170] and monitoring systems.

In order to comprehend different regulatory approaches in this regard, the following part of this paper will be devoted for analysing requirements set in the Estonian AML law. The analysis itself will emphasize differences and methodologies used for regulating virtual currency service providers, thus giving an overview of what are the possible solutions to ensure effective compliance. Having understood that, comparison between Latvian and Estonian approaches will be established, thus elaborating on aspects, which can be considered as tailored/applicable and which might not.

2.3. AML minimum regulatory requirements in Estonian legal system in regards to the virtual currency service providers

Beforehand minimum requirements set in the Latvian legal framework were discussed and analyzed, thus emphasizing approach taken by the respective supervisory authority. As it was clarified, virtual currency service providers in Latvia were rendered as the subjects of the law without applying tailored risk assessing mechanisms. Due to the fact, that this kind of economic activity underlines great pile of anonymity concerns, more tailored approach would benefit both - supervisory authority and the subject itself. On the other hand, Latvian SRS has provided little guidelines in this regard besides general clarification material, therefore virtual currency service providers lacks soft law instruments in order to effectively establish numerical risk scoring system considering particular identified risk indicators, for instance.

The rationale behind examining Estonian legislative framework in regards to the AML provision thrives from the beneficial economic and regulatory environment[171], which attracts foreign investors and allows them to proceed with their business models and visions. Due to the fact that Estonian regulatory framework is quite fintech friendly, for the sake of the analysis their implemented AML virtual currency service provider's requirements will be examined in a detail.

2.3.1. Supervisory authority

As per following the same skeleton introduced previously, the analysis will be started by explaining legal basis related to supervisory authority's competence. Importance of mentioning it stems from the fact that sound internal governance at some extent derives from sound supervision framework[172], therefore the author of this thesis stipulates and reinforces the core and initial argument by providing comprehensive sector overview.

Credit institutions, as well as financial institutions in general in Estonia are supervised by the Estonian Financial Supervision and Resolution Authority (in Estonian -

[169] *Ibid*, 5.1.2.

[170] Kristīna Loboda, Sliekšņa deklarācijas – kam un kā tās būs jāiesniedz, 02.12.2019, Available at https://lvportals.lv/skaidrojumi/311016-slieksna-deklaracijas-kam-un-ka-tas-bus-jaiesniedz-2019, Accessed on 05.05.2020.

[171] OECD, Economic Survey of Estonia (December 2019), p. 4, Available at https://www.oecd.org/economy/estonia-economic-snapshot/ ,Accessed on 05.05.2020.

[172] Grant Kirkpatrick, The Corporate Governance Lessons from the Financial Crisis, OECD, 2009, p. 26, Available at https://www.oecd.org/finance/financial-markets/42229620.pdf, Accessed on 05.05.2020.

Finantsinspektsioon) (hereinafter referred to as the "FSA"). Institution itself is seeking to enhance "the stability, reliability, transparency and efficiency of the financial sector"[173]. As it was mentioned above, one of the supervised sector is financial institutions, hence according to the Money Laundering and Terrorist Financing Prevention Act (hereinafter referred to as the "Estonian AML law") Article 2 paragraph 5, which stipulates that "The provisions of this Act governing financial institutions apply to virtual currency service providers [...]."[174], virtual currency service providers should be treated as classical financial institutions, meaning that relatively similar requirements are directly binding to these subjects of the law. This, however, establishes grounds for more unified approach for the FSA to govern and protect integrity of the Estonian financial sector.

Eventually, such requirement indeed hinders compliance requirements due to the fact that related FSA passed recommendations and additional provisions in regards to the financial institutions are now also directly applicable to the virtual currency service providers, unless otherwise stated. Particular set of procedural provision increases not only the regulatory burden, but also related system and procedure creation and performance costs since additional manpower and resources ought to be needed for proper maintenance matters.

On the other hand, as it was mentioned previously, unified governance ensures more efficient supervision mechanism since requirements, which must be met and respected, are almost equal to all subjects of the law. Thus the element of risk-based perception and interpretation of the law is excluded, which leads to avoiding potential opportunities to fictitiously create compliance gaps.

2.3.2. Scope of the law and key defining terms

Due to the fact, that it is up to each MS to interpret the law in accordance with its own risk perception, relevant terminology should also be emphasized in order to comprehend the existing regulatory scope and perspective.

Estonian AML law introduces virtual currencies and related elements similarly as in the case of Latvia:

> **virtual currency** means a value represented in the digital form, which is digitally transferable, preservable or tradable and which natural persons or legal persons accept as a payment instrument, but that is not the legal tender of any country or funds [...][175]
>
> And
>
> **virtual currency exchange service** means a service with the help of which a person exchanges a virtual currency against a fiat currency or a fiat currency against a virtual currency or a virtual currency against another virtual currency[176][177]

[173] Article 31, Financial Supervision Authority Act, Available at https://www.riigiteataja.ee/en/eli/515012020001/consolide , Accessed on 06.05.2020.
[174] Article 25, Money Laundering and Terrorist Financing Prevention Act, Available at https://www.riigiteataja.ee/en/eli/ee/511122019005/consolide/current , Accessed on 06.05.2020.
[175] *Supra* note 174, Article 3 Para. 9.
[176] *Ibid*, Para. 10^1.
[177] Virtual currency exchange service providers in the Estonian AML law are also referred simply as the "virtual currency service".

As it is observable, virtual currency exchange service providers are categorized into three sub-subjects stipulating following economic activity:

1. Virtual currency exchange to a fiat currency[178];
2. Fiat currency exchange to a virtual currency[179];
3. Virtual currency exchange to another virtual currency[180].

Also, as in the case of Latvia, virtual currency wallet service providers are considered as the relevant subjects of the law, thus having the same regulatory requirements as in the case of virtual currency exchange service providers.

However, since this thesis is limited in its scope to analyze only virtual currency exchange service providers, the FSA has clarified that virtual currency "mining"[181] activities are not part of the supervision, thus are not required to be compliant with the AML requirements and provisions[182]. Therefore, for the avoidance of doubt, companies, which ensures virtual currency mining activities, should pay attention to taxation aspects and relevant provisions[183].

2.3.3. Minimum requirements set in the Estonian AML law

For the purposes of this section, the author seeks to clarify and analyze minimum requirements set by the Estonian AML law in regards to the virtual currency exchange service providers. As it can be established already and taking into account the fact that Estonia provides beneficial regulatory and market conditions for innovative and new businesses, the author of this thesis expects seeing minor, but at the same time crucial regulatory differences compared to the Latvian AML law.

Previously it was already established that virtual currency exchange service providers are considered as the financial institutions[184], therefore regulatory requirements in this regard are also applicable to them. Following above introduced structure, the first outlined element touches upon the registration requirement.

According to the General Part of the Economic Activities Code Act (hereinafter referred to as the "GPEACA"), all undertakings, whose economic activity is not an exception prescribed by the GPEACA[185], are required to register their activity to Economic administrative authority[186]. Nevertheless, in addition to that, Article 70 of the Estonian AML

[178] *Supra* note 174, Article 3 Para. 10^1.
[179] *Ibid.*
[180] *Ibid.*
[181] „Mining - Cryptocurrency mining is the process in which transactions between users are verified and added into the blockchain public ledger.", Binance Academy, What is Cryptocurrency Mining?, Available at https://www.binance.vision/blockchain/what-is-cryptocurrency-mining, Accessed on 06.05.2020.
[182] Financial Supervisory Authority, Which regulations apply to this activity, Information for entities engaging with virtual currencies and ICOs, Available at https://www.fi.ee/en/investment/aktuaalsed-teemad-investeerimises/virtuaalraha-ico/information-entities-engaging-virtual-currencies-and-icos , Accessed on 06.05.2020.
[183] *Ibid.*
[184] *Supra* note 173.
[185] Article 2, General Part of the Economic Activities Code Act, Available at https://www.riigiteataja.ee/en/eli/530102013062/consolide , Accessed on 06.05.2020.
[186] *Ibid,* Article 7.

Law requires virtual currency exchange service providers to obtain supplementary license[187] from the FSA[188].

In theory as well as in practice, acquisition of a license indicates that particular service provider/business operator has expressed an incentive to operate accordingly to the law, thus acquisition of a license puts on a reputational stamp to said company. For the customer, recognition of a license increases the level of trustworthiness and dependence on particular institutions provided services or business model.

By elaborating on aforementioned, in order to receive a license from the FSA, virtual currency exchange service provider is required to follow requirements set in the Estonian AML Law (specifically - Article 70 and 72). Notwithstanding that, there are some straightforward requirements, which limits non-resident possibilities to maintain economic activity in Estonia, for instance, if any of involved person (both legal and natural) in the virtual currency exchange service company is considered as non-resident, certificate of the criminal records database must be authenticated by a notary[189] and submitted to the FSA. Additionally, in order to even perform economic activity, the registered seat, the seat of the management board and place of business must be in Estonia[190]. Also reputation, capital and other requirements are posed as mandatory provisions to virtual currency exchange service providers.

Particular licensing requirements sets high barrier for these subjects, thus increasing the compliance costs. Considering that part of them came into force on March 2020, the conclusion can be derived that impact stemming from 5th AML directive is quite substantial, therefore developed requirements/mechanisms seeks to mitigate any potential and existing risks.

One of the reasons, why such requirements in general are introduced could stem from the fact that Danske bank branch, which was registered in Estonia, was involved in significant money laundering scandal, where estimated 200 billion EUR were funneled through Estonian financial system using said branch[191]. Although a bank essentially is not the same concept as virtual currency exchange institution, reputational damage has been done and effective further risk mitigation mechanisms could renew the integrity of the Estonian financial system (regardless that Basel institute of governance has ranked Estonia as the most safest country in terms of ML amongst 125 other countries[192]). On the other hand, the number of issued licenses from until 2017[193] to virtual currency service providers in Estonia was sky rocking, indicating that the law within the time was too informative and less efficient in regards to

[187] *Supra* note 174, Article 70.
[188] *Ibid*, Article 71.
[189] *Ibid*, Article 70^{38}.
[190] *Ibid*, Article $72^{1}4$.
[191] Teis Jensen, Explainer: Danske Bank's 200 billion euro money laundering scandal, Reuters, 19.11.2018, Available at https://www.reuters.com/article/us-danske-bank-moneylaundering-explainer/explainer-danske-banks-200-billion-euro-money-laundering-scandal-idUSKCN1NO10D, Accessed on 07.05.2020.
[192] International Centre for Asset Recovery, Basel AML Index 2019 A country ranking and review of money laundering and terrorist financing risks around the world, August 2019, Available at https://www.baselgovernance.org/sites/default/files/2019-08/Basel%20AML%20Index%202019.pdf, Accessed on 02.05.2020.
[193] Rahapesu ja terrorismi rahastamise tõkestamise valitsuskomisjoni analüüs ja ettepaneku, 2018, p. 14, Available at https://www.rahandusministeerium.ee/sites/default/files/rahapesu_tokestamise_valitsuskomisjoni_analuus_ja_ettepanekud.pdf, Accessed on 07.05.2020.

regulatory supervision. It provided attractive thresholds, which did not impose any difficulties for passing them[194].

Moreover, due to the fact that FSA has the authority to issue operational licenses, it also has the right to revoke them in case if it finds legitimate reason for such action[195] or there has been a compliance violation,[196] which underlines great pile of threats. Specific, subject oriented license revocation has not been specified in the respective law, therefore it can be concluded that subjects, which are specified in Article 70[197], can get their licenses revoked by the FSA.

On the one hand, in order to maintain economic activity by providing virtual currency exchange services, the AML 5th directive sets a requirement to register in each operating MS. Concluding that licensing requirements are much stricter than registration (if there are any), the reliance concern raises. Comprehending the synergy between both, it would make sense that, if particular company, operating as a virtual currency exchange service provider, has obtained the license in one state, which is a part of the EU (therefore theoretically having integrated the same applicable legislative mechanisms), its recognition in other should at least at the minimum, give more beneficial circumstances in order to establish economic activity there. Nevertheless, stemming directly from the Estonian AML law, there are no requirements, which would allow or which would refuse such action, however, the Estonian government has clarified that reliance on licenses issued outside Estonia is not possible[198].

Since virtual currency exchange service providers are considered as the financial institutions (from the Estonian AML law point of view), there are additional and more straight forward requirements to which the particular subject must be compliant. Having identified and analyzed provisions governing licensing and registering, supplementary ones, which touches upon internal control system, risk appetite and *etc*., will also be perceived by the scope of this thesis.

As in the case with financial institutions, current legislative framework seeks virtual currency exchange service providers to establish effective risk management system[199], which must be reinforced by clarifying and identifying preliminary threats stemming from used products, geographies involved and *etc*.[200]. Accumulated result, in theory, must serve the purpose for proposing an efficient risk detection mechanism, which supplements and "guides" institution's daily operations. Due to the fact that the business model itself is quite risky in terms of risk management or stability, respective institutions should be very strict and wise in their decisions, while agreeing on tolerable risk. For instance, delivery channel (which is one of the key components of risk management strategy) should be clearly defined, *e.g.* whether the potential customer will be able to utilize only online service or also specified ATMs are

[194] *Ibid.*
[195] *Supra* note 174, Article 75.
[196] *Ibid*.
[197] *Ibid*, Article 60 (1- 6).
[198] Police and Border Guard Board, Cross Border Operation, Activity licence for the provision of financial services, Available at https://www.eesti.ee/en/licences-and-notices-of-economic-activity/financial-activities/activity-licence-for-the-provision-of-financial-services/ , Accessed on 07.05.2020.
[199] *Supra* note 174, Article 14.
[200] *Supra* note 174, Article 13.

going to be used[201]. The same analogy would be attributable to the identification process, *e.g.*, to what extent non face-to-face identification can be tolerated[202].

Moreover, regulatory provisions, *inter alia*, also pushes virtual currency exchange service providers to establish risk appetite[203], which must be prepared by the institution's senior management[204]. As per it is clarified by the same article, virtual currency exchange service provider is requested to presume its potential customer[205] and tolerable risk profile. By elaborating on potential customer profile, it has also been stated that in case with:

1) Foreign national[206]

2) Person residing outside the European Economic Area (hereinafter referred to as the "EEA")[207]

3) Natural person, whose transaction volume exceeds 15 000 EUR per calendar month[208]

4) Legal person, whose transaction volume exceeds 25 000 EUR per calendar month[209]

Only two identification scenarios (by using information technology means) are possible - either by concluding face-to-face identification[210] or by showing an ID card issued by following states[211]:

1) Germany

2) Italy

3) Croatia

4) Estonia

5) Spain

6) Luxembourg

7) Belgium

8) Portugal

---

[201] FINTRAIL, Assessing Risk, Cryptocurrencies: Getting Serious About Financial Crime Risk Management, A FINTRAIL White Paper, August 2018, Available at https://static1.squarespace.com/static/5b9798661aef1d8112a02bd0/t/5c0d5ad9562fa76785391c0b/1544379105284/Fintrail+Cryptocurrencies+WP+2018+280818.pdf , Accessed on 08.05.2020.

[202] *Supra* note 35, Delivery channels, p. 41.

[203] *Supra* note 174, Article 10.

[204] *Ibid.*

[205] *Ibid.*

[206] *Ibid,* 31 article.

[207] *Ibid*.

[208] *Ibid.*

[209] *Ibid.*

[210] Lextal, The Estonian crypto regulation faces a lethal challenge, Available at https://lextal.ee/en/the-estonian-crypto-regulation-faces-a-lethal-challenge/, Accessed on 09.05.2020.

[211] Electronic identification schemes notified pursuant to Article 9(1) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2019.425.01.0006.01.ENG&toc=OJ:C:2019:425:TOC#ntc1-C_2019425EN.01000601-E0001, Accessed on 09.05.2020.

9) United Kingdom

10) Czech Republic

11) The Netherlands

12) Slovakia

13) Latvia

This, however, creates a challenge for maintaining an effective business model. The virtual currency exchange service provider is now practically forbidden to provide its services to persons, who are considered as non-residents and do not have an ID card issued in aforementioned jurisdictions due to the fact that it would be highly unpractical for them to obtain either a legally binding document issued in country other than their residence one or e-residence card issued in Estonia. Indeed, theoretically, such option of course exists (to have these types of persons as customers), although in practice there would be a small number of persons ready to engage in such bureaucratic procedure. The same requirement applies to customers, who have already established a relationship with the virtual currency exchange service provider, which has acquired respective license prior these requirements came in force, thus currently they have an obligation to renew their license prior 1st of July, 2020[212].

Furthermore, the due diligence measures, including identification of the customer, monitoring of business relationship, EDDs, SDDs are also a part of the virtual currency exchange service provider regulatory scope.

By slightly elaborating on previously mentioned, in general, the due diligence categorizes in two segments - upon the establishment of a business relationship[213] and during the ongoing monitoring of it[214]. These measures must be tolerated in order to fulfil obligations set by the KYC principles for the whole period, whenever the virtual currency exchange service provider has a practical or theoretical relationship with the customer. *Inter alia*, identification and verification requirements, nevertheless, have not been tailored for the purpose of particular subjects of the law, however, since the financial institution element is compatible in this situation, requirements stemming from the law of "Requirements and procedure for identification of persons and verification of person's identity data with information technology means"[215] must be implemented in their internal procedures, thus displaying compliance with this normative act as well.

Both EDD and SDD approaches can be used in order to examine a customer, however, the EDD must be applied in situations whereas the risk has been identified as higher-than-usual[216]. Whilst SDD can be applied only when the customer has been scored with the risk

[212] *Supra* note 174, Article 118^2.

[213] [213] Financial Supervisory Authority, Article 4.1.3, Advisory Guidelines of Finantsinspektsioon "Organisational solutions and preventive measures for credit and financial institutions to take against money laundering and terrorist financing", p. 25, Available at https://www.fi.ee/sites/default/files/2019-01/FI%20rahapesu%20t%C3%B5kestamise%20juhend%202018%20%28EN%29_pdf.pdf , Accessed on 10.05.2020.

[214] *Ibid*.

[215] Requirements and procedure for identification of persons and verification of person's identity data with information technology means, Available at https://www.riigiteataja.ee/en/eli/509012019003/consolide , Accessed on 10.05.2020.

[216] *Supra* note 174, Article 36.

rating of low[217]. Given the fact, that virtual currency business constitutes higher risk than any other businesses, the SDD approach, although in theory would be possible, in practice should not be applied, unless the institution has adopted "step-ahead" requirements, which are much stricter than established in the national legislation, thus ensuring developed compliance mechanism for clearing out customers, who possess a relatively smaller risk for financial institutions in general, but higher risk for virtual currency service providers.

The last requirement, to which virtual currency exchange service provider must be compliant, is an obligation report to the FIU if the suspicious activity/transaction has been identified[218]. The process must be done in accordance with the Estonian AML Law and FSA issued guidelines on the same matter[219]. Suspicious characteristics, however, has been listed in the additional document[220], which has been issued by the Police and Border Guard Board of Estonia. Notwithstanding the scope designated for the financial institutions, there are specifically tailored characteristics, which are compatible with virtual currency exchange service providers.

[217] *Ibid*, Article 32.
[218] *Ibid*, Article 49.
[219] Minister of the Interior, Guidelines for Submitting A Report To The Financial Intelligence Unit, Available at https://www.politsei.ee/files/Rahapesu/rahapesu-andmebueroole-esitatava-teate-esitamise-juhend-en.pdf?eead45cee2 , Accessed on 11.05.2020.
[220] Financial Intelligence Unit, Guidelines on the characteristics of suspicious transactions, Police and Border Guard Board, Available at https://www.politsei.ee/files/Rahapesu/juhend-kahtlaste-tehingute-tunnuste-kohta-en.pdf?3e4fc8c9fe, Accessed on 11.05.2020.

3. LATVIAN AML LAW MINIMUM REQUIREMENT COMPARISON TO ESTONIAN AML LAW MINIMUM REQUIREMENTS

The second chapter identified what the minimum requirements set in respective Estonian and Latvian legislation in regards to the virtual currency exchange service providers are. By having emphasized theoretical application against the practical one, the author of this thesis used the best industry practice as well as fictitious scenarios throughout which potential gaps and further non-compliance might arise.

The purpose of this chapter is to give a comparative overview of how large the regulatory burden might be if the person decides to operate its virtual currency exchange service business in one or another country. A fictitious scenario will be used to elaborate on the pros and cons of stemming from both legal systems.

Let's suppose that there is a company X, which considers entering the Baltic market and operate as virtual currency exchange service provider, however, it has not yet decided, at which particular state it must register the legal person. There are two options - Estonia or Latvia. Therefore the first aspect touches upon the registration.

As it was analyzed in the thesis, in Latvia the requirement is to register virtual currency exchange service provider's economic activity without obtaining any license or authorization document, whilst in Estonia, it is an obligation to obtain one. This, however, raises two additional concerns - Estonian regulatory framework seeks to be more costly since the institution has to pay a fee of 3 300 EUR for receiving a license[221] (previously it was 345 EUR). In addition, due to the fact that operational license is required, in case if it gets revoked, the institution may not pursue with its business activity in Estonia anymore. Thus both - reputational and financial damage could be faced. As per understanding that by receiving a license, sort of classification is attributed, the virtual currency exchange service provider in Estonia will be considered as the financial institution, *i.e*. all the regulatory requirements regulating financial institutions in regards to the AML will be applicable to the virtual currency exchange service provider. Also, in Estonia, the senior management is required to submit an extensive load of good-reputation ensuring documents in order to ensure that particular business will not be used in order to facilitate ML,

Nevertheless, this on the other hand also provides clarity and a unified approach towards equal regulatory treatment and further issuing any guidelines or recommendations. Basically - whenever there will be uncertainty about how the law should be interpreted in case of virtual currency exchange service providers, the general consideration will be derived from comprehending the scope of financial institutions, nonetheless, such interpretation also could lead to lack of efficient regulation since virtual currency exchange service providers are not perceived as a single and unique subject of the law.

Moreover, comprehending the next regulatory requirement, in Latvia as well as in Estonia, virtual currency exchange service provider is subjected to establish an internal control system and, therefore, internal risk assessment. Since in both jurisdictions virtual currency exchange service providers are considered as high-risk business operators, attitude,

[221] Maarja Lehemets, New crypto rules – stricter requirements for virtual currency service providers in Estonia, 05.03.2020, Available at https://triniti.eu/2020/03/05/new-crypto-rules-stricter-requirements-for-virtual-currency-service-providers-in-estonia/, Accessed on 12.05.2020.

which thrives from banks, for instance, might be similar in both jurisdictions in case if a willingness to open a company's bank account occurs. Although, given the fact, that in Estonia virtual currency exchanges are treated as financial institutions, overall risk perception could be more supportive since in theory credit institutions should be aware of the regulatory requirements and potential treatment from the supervisory authority towards the financial institutions, thus virtual currency exchange service providers.

Elaborating on previously mentioned, Swiss credit institutions, notwithstanding the fact that Switzerland has a beneficial environment for virtual currency businesses[222], also are protective in terms of building a relationship with such service providers[223], however, the future with such market participants is inevitable, thus robust and strict due diligence requirements are expected to guide onboarding experience for virtual currency businesses.

By emphasizing internal systems as such, again, in case of Latvia, there are general requirements and almost no guidance at all on how to create specific and even tailored control system or risk assessment. Indeed, the SRS, being as the supervisory authority, has issued one document in relation to the AML compliance, however, comparing to the pile of recommendations and guidelines issued by the FCMC for credit institutions, for instance, it may appear as insufficient in terms of regulating such market participants.

On the contrary - Estonian approach on the same regard is more comprehensive than it is in the case with Latvia since the common denominator of financial institution exists. This eventually means, that issued guidelines, recommendations and other binding legal acts could be treated as supplementary tools since general clarifications or elaborations are expected to be more convenient to establish aforementioned systems. Although, as it was mentioned, such situation arises only by comparing to Latvia's example, because still tailored requirements are missing and detailed clarification, specifically designated for such service providers, are not yet introduced in both legal systems. By extending the scope of internal risk assessment, the virtual currency exchange service provided under Estonian AML law is required to draft a risk appetite statement and as it was discussed previously, such statement seeks to give a clear tone from the top motto, which sets institution's tolerable level of risks. Although, since it has not been required by Latvian AML law requirements, it does not mean that virtual currency exchange service provider cannot establish one for itself in order to clearly define its risk capacity to achieve its strategic objectives and business plan[224]. It, eventually, could be considered as a good internal communication channel amongst employees, which maintains an up-to-date mindset of what are the institution's goals on overseeing future.

By comparing due diligence requirements, *inter alia*, identification, verification, transaction monitoring, KYC, EDD, SDD, they are relatively same in regards to virtual currency exchange service providers. Both jurisdictions have considered overall approach, therefore there are no major differences. The common theme is that the virtual currency

[222] Daniel Haeberli, Stefan Oesterhelt, Alexander Wherlock, Switzerland, Blockchain & Cryptocurrency Regulation 2020, Available at https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/switzerland, Accessed on 13.05.2020.

[223] EY, AML due diligence requirements from a Swiss banking perspective, Cryptocurrencies, September 2019, p. 4, Available at https://www.eycom.ch/en/Publications/20191001-Cryptocurrencies-AML-due-diligence-requirements-from-a-Swiss-banking-perspective/download, Accessed on 10.05.2020

[224] Financial Stability Board, Risk Appetite Definition, Principles for An Effective Risk Appetite Framework, Available at https://www.fsb.org/wp-content/uploads/r_131118.pdf, Accessed on 10.05.2020.

exchange service provider is required to know its customer, business relationships and aggregate existing scope of the aforementioned. As per comprehending that one of the critical components of the whole due diligence scope touches upon the transaction monitoring, both jurisdictions could ensure blockchain algorithmic approach, which detects particular patterns, characteristics[225] and if, historically, particular blockchain account has been associated with the criminal nature/activity, integration of automated such account recognition[226]. EDD, SDD and identification requirements are relatively similar, although in case of Estonia if the institution is willing to have a business relationship with a customer, who is considered as a non-resident, he/she will have to acquire additional legal documentation (from either Estonia itself or "partnering" countries), which would allow meeting regulatory requirements set by the Estonian AML law. This process, in practice, is quite unattractive, therefore business expansion by involving a variety of non-resident customers will be limited, and thus financial benefit could be lost.

Furthermore, by comparing obligation to report, both jurisdictions have imposed similar requirements in this regard. Mainly, whenever the institution detects a suspiciousness regarding the activity or financial transaction, it must immediately report it to the respective FIU. The difference, however, arises in case of Estonia, since virtual currency exchange service providers should rely on already identified characteristics (since financial institution element comes into play), although given the complexity of the business model itself, the institution must establish more tailored characteristics to its economic activity in order to be more compliant, thus ensuring more efficient internal governance framework.

Eventually, the last aspect, which requires comparison, touches upon the supervisory authority's element. In Latvia, there are in total 4 supervisors, which are responsible for the specific subject of the law supervision. While *Latvijas Banka* supervises foreign currency exchange service providers (which economic activity is similar to the virtual currency exchange service providers), the SRS, on the other hand, is responsible for supervising virtual currency exchange service providers. As it was discussed previously in the paper, this from the logical point of view seems rather unusual since both have a relatively similar concept of economic activity. Therefore different perspectives and interpretation methods could be observed. In case of Estonia, subjects of the law are supervised by one authority, *i.e*. the FSA. This type of supervision ensures consistency and efficiency in terms of unified approach as well as there are no interpretation gaps between multiple supervisors, as it is in case of Latvia.

By considering all compared requirements, general remark can be established that from the business point of view, Latvia seems more attractive since there is a wide room for interpretation left. Although, it also means, that since there is almost no practical experience in regulating these market participants, the first audited service providers will emphasize the overall picture of how they are getting along with the compliance matters. In case of Estonia, although the first impression might seem as cost-driving, the regulatory burden might ensure higher compliance, thus risk mitigation mechanisms will be tolerated with higher deference. The decision to enter the particular market should be based on understanding whether the

[225] Sherri Scott, Transaction Monitoring Cryptocurrency compliance: An AML perspective, 2018, p. 8, Available at https://fraudfighting.org/wp-content/uploads/2018/05/Cryptocurrency_Compliance_An_AML_Perspective_S.Scott_.pdf , Accessed on 11.05. 2020.
[226] *Ibid.*

company wants to make a profit or it wants to be sure that less risky transactions go through its internal financial systems.

Conclusion

By referring back to the initially asked research question "To what extent minimum requirements set in Latvian and Estonian AML law are attributable to the virtual currency exchange service providers?" the answer is divided in two parts.

As per comprehending the minimum requirements stemming from the Latvian AML law, concluding marks are as follows. Among the other things, it appears that the approach used in order to subject virtual currency service providers is quite formal, meaning that there are no strict guidelines or even tailored requirements introduced by the legislator/supervisory authority in order to prevent financial crime in a particular sphere. Such a notion rises substantive concerns about the efficiency and compatibility of compliance, thus leading to possible fines from regulator and failure to ensure adequate mechanisms in this regard. Moreover, understanding that first regulatory analysis/results on virtual currency service providers will be available only in late 2020 or early 2021, ignorance of acceptable compliance program will be actual and relevant since there are no examples of how it should be operated or maintained, therefore this "pilot" year may disclose and emphasize legislative gaps and cornerstones.

On the other hand, virtual currency exchange service providers under Estonian AML law have been treated as financial institutions. Such categorisation, from the author's perspective, is neither effective nor incapable. On the one hand, by imposing the same requirements as financial institutions have, the regulatory framework for virtual currency business, in general, is more straightforward and consists of strict obligations to which it must be compliant. It indeed gives more structured approach, which must be considered prior investing in such business opportunity. Even banks, for instance, prior opening accounts for these service providers, in theory, are ensured that their business model is regulated and should be in line with requirements set in the respective law, however the underlined risk still is quite high and in some cases - impossible to tolerate[227]. And this, eventually, rises other concern - even by being compliant to the requirements designated for the financial institutions, more tailored approach is still missing. The law itself and assigned recommendations are not focusing on giving a tailored regulatory framework, which would be suitable to ensure, firstly, compliance matters for virtual currency exchange service providers and secondly, reasonable environment to operate in this business sector.

Therefore, the general conclusion can be established - both jurisdictions lack tailored requirements and guidance's, which would allow these subjects to ensure technical compliance at its utmost notion. In theory, formal requirements exist to which these particular subjects must be compliant, however, in practice, there could arise a variety of unanswered questions and misinterpreted regulatory concepts.

As per elaborating on the second research question "Which of the above-mentioned jurisdictions provides more beneficial environment to operate a virtual currency exchange

[227] Josias Dewey, Andrew Schofield, Suzie Levy, Caroline Collingwood, Alan Falach, Rory Smith, Blockchain & Cryptocurrency Regulation 2019 Contributing Editor Josias Dewey, p. 279, Available at https://www.acc.com/sites/default/files/resources/vl/membersonly/Article/1489775_1.pdf, Accessed on 12.05.2020.

service requirement business?", the answer should be perceived by either looking from the business or legal point of view.

The business point of view suggests that Latvia is more attractive in terms of establishing a virtual currency exchange service providing company since the regulatory burden is not as costly as it is in case of Estonia. Latvia provides more general requirements, which, although will increase costs for a particular subject of the law, will not accumulate a very high expense report. Estonia, on the other hand, already starts being costly by imposing a licensing requirement, for instance, therefore the monetary factor comes not only in, but also further reputational one must be considered alongside with the previous.

Subsequently, the analysis and provided evidence ensured that Estonian imposed regulatory framework, since being derived from the financial institution perspective, implies that there is several additional requirements, which are not considered by Latvian legislator, for instance.

This, however, leads to the second point of view - legal. Estonian regulatory obligations are stricter then they are compared to Latvian, therefore the business side does not have a substantial benefit in this regard. Admittedly, Latvia might seem as a pleasant environment at first glance, however regulatory requirements in Estonia provides more clarity and trustability of the sector in general. Since the treatment stems from financial institutions, it could be expected that the same compliance standards will be respected.

Bibliography

Primary sources

1. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.
2. DIRECTIVE (EU) 2018/843 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.
3. Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.
4. Financial Supervision Authority Act, Available at https://www.riigiteataja.ee/en/eli/515012020001/consolide , Accessed on 06.05.2020.
5. Finanšu un kapitāla tirgus komisijas 2018. gada 9. janvāra noteikumi Nr. 3 "Klientu padziļinātās izpētes normatīvie noteikumi kredītiestādēm un licencētām maksājumu un elektroniskās naudas iestādēm". Latvijas Vēstnesis, 10, 15.01.2018, Available at https://likumi.lv/ta/id/296439/redakcijas-datums/2018/06/02. Accessed on 06.04.2020.
6. General Part of the Economic Activities Code Act, Available at https://www.riigiteataja.ee/en/eli/530102013062/consolide , Accessed on 06.05.2020.
7. Judgment of the Court (Fifth Chamber) of 22 October 2015, Skatteverket v David Hedqvist, Request for a preliminary ruling from the Högsta förvaltningsdomstolen, Case C-264/14. Para. 28-31, Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0264, Accessed on 20.04.2020.
8. Law on Personal Income Tax (Likums "Par iedzīvotāju ienākuma nodokli"), Latvijas Vēstnesis, 32, 01.06.1993. Available at https://likumi.lv/ta/id/56880, Accessed on 20.04.2020.
9. Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing (Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma un proliferācijas finansēšanas novēršanas likums), Available at https://likumi.lv/ta/id/178987, Accessed on 20.04.2020.
10. Law on the Procedure for Introduction of Euro (Euro ieviešanas kārtības likums), Latvijas Vēstnesis, 33, 15.02.2013, Available at https://likumi.lv/ta/id/254741, Accessed on 28.04.2020.
11. Ministru kabineta 2019. gada 27. augusta noteikumi Nr. 407 "Noteikumi par sliekšņa deklarācijas iesniegšanas kārtību un saturu". Latvijas Vēstnesis, 182, 06.09.2019, Available at https://likumi.lv/ta/id/309171, Accessed on 05.05.2020.
12. Money Laundering and Terrorist Financing Prevention Act, Available at https://www.riigiteataja.ee/en/eli/ee/511122019005/consolide/current , Accessed on 06.05.2020.
13. REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

14. Requirements and procedure for identification of persons and verification of person's identity data with information technology means, Available at https://www.riigiteataja.ee/en/eli/509012019003/consolide , Accessed on 10.05.2020.

15. Sanction Risk handling rules (Sankciju riska pārvaldīšanas normatīvie noteikumi), Available at https://m.likumi.lv/doc.php?id=304787 , Accessed on 05.05.2020.

Secondary sources

1. ACAMS, Understanding the new DFS Part 504 Regulations and the Associated AML Program testing Challenges, p. 16, Available at http://files.acams.org/pdfs/2017/Understanding_the_New_DFS_Part_504_Regulations_C.Recor.pdf , Accessed on 05.05.2020.

2. Adrian, Tobias, Tommaso Mancini Griffoli, The rise of digital money, International Monetary Fund 2019, 15.07.2019, p. 6, Available at https://www.imf.org/en/Publications/fintech-notes/Issues/2019/07/12/The-Rise-of-Digital-Money-47097, Accessed on 08.04.2020.

3. AirBaltic, AirBaltic - World's First Airline To Accept Bitcoin, Riga, 22.07.2014, Available at https://www.airbaltic.com/airbaltic-worlds-first-airline-to-accept-bitcoin, Accessed on 18.04.2020.

4. Appendix 1, Risk factor No. 4., Finanšu un kapitāla tirgus komisijas 2019. gada 21. augusta noteikumi Nr. 135 "Klientu izpētes, klientu padziļinātās izpētes un skaitliskā riska novērtējuma sistēmas izveides normatīvie noteikumi". Latvijas Vēstnesis, 176, 29.08.2019. https://likumi.lv/ta/id/309047, Accessed on 08.04.2020.

5. BaFin, Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer, 19.12.2013, Available at https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2014/fa_bj_1401_bitcoins.html, Accessed on 15.04.2020.

6. Basel Committee on Banking Supervision, Principles for enhancing corporate governance October 2010, Available at https://www.bis.org/publ/bcbs176.pdf, Accessed on 30.04.2020.

7. Bech, Morten, Rodney Garratt, Central bank cryptocurrencies, BIS Quarterly Review, September 2017 Available at https://www.bis.org/publ/qtrpdf/r_qt1709f.pdf, Accessed on 09.04.2020.

8. Bijsterveld, Sophie van, Section 5, Transparency In The European Union: A Crucial Link In Shaping The New Social Contract Between The Citizen And The Eu, Available at https://www.ip-rs.si/fileadmin/user_upload/Pdf/clanki/Agenda__Bijsterveld-Paper.pdf Accessed on 05.04.2020.

9. Blanc, Florentin, Ernesto Franco-Temple, Introducing a risk-based approach to regulate businesses, how to build a risk matrix to classify enterprises or activities, Nuts & bolts. Washington, DC, World Bank Group, 2013, Available at http://documents.worldbank.org/curated/en/102431468152704305/Introducing-a-risk-based-approach-to-regulate-businesses-how-to-build-a-risk-matrix-to-classify-enterprises-or-activities, Accessed on 05.04.2020.

10. Blockchain.com, Total Circulating Bitcoin, Available at https://www.blockchain.com/charts/total-bitcoins , Accessed on 16.04.2020.

11. Canelon, Luis, Carl Hatfield, Chetan Shah, Anti-money laundering transaction monitoring system implementation considerations, 31.05.2013, https://www.acamstoday.org/anti-money-laundering-transaction-monitoring-system-implementation-considerations/, Accessed on 02.05.2020.

12. Central bank of Latvia, Ārvalstu valūtu skaidrās naudas pirkšanas un pārdošanas sektora noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas risku novērtējums, 2019, p. 3-4, Available at https://www.bank.lv/images/stories/pielikumi/valutasmaina/Sektorialais-risku-novertejums-Latvijas-Banka-02042019.pdf , Accessed on 27.04.2020.
13. Deloitte, The Fourth EU Anti Money Laundering Directive, 2015, Available at https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/FinancialServices/investmentmanagement/ie_2015_The_Fourth_EU_Anti_Money_Laundering_Directive_Deloitte_Ireland.pdf, Accessed on 24.04.2020.
14. Dewey, Josias, Andrew Schofield, Suzie Levy, Caroline Collingwood, Alan Falach, Rory Smith, Blockchain & Cryptocurrency Regulation 2019 Contributing Editor Josias Dewey, p. 279, Available at https://www.acc.com/sites/default/files/resources/vl/membersonly/Article/1489775_1.pdf, Accessed on 12.05.2020.
15. Dyson, Simon, William J Buchanan, Liam Bell, The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime, 29.07.2019, p. 2 , Available at https://arxiv.org/pdf/1907.12221.pdf, Accessed 11.04.2020.
16. Draft Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (‘’The Risk Factors Guidelines’’), amending Guidelines JC/2017/37 TRANSACTION MONITOIRNG Accessed on 05.04.2020.
17. EBA, Consultation paper, Draft Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (‘’The Risk Factors Guidelines’’), amending Guidelines JC/2017/37, 5 February 2020, Available at https://eba.europa.eu/sites/default/documents/files/document_library/Publications/Consultations/2020/Draft%20Guidelines%20under%20Articles%2017%20and%2018%284%29%20of%20Directive%20%28EU%29%202015/849%20on%20customer/JC%202019%2087%20CP%20on%20draft%20GL%20on%20MLTF%20risk%20factors.pdf, Accessed on 08.04.2020.
18. EBA, EBA Opinion on ‘virtual currencies’, 4 July 2014, Available at https://eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1, Accessed on 15.04.2020.
19. EBA, EBA warns consumers on virtual currencies, 12 December 2013, Available at https://eba.europa.eu/eba-warns-consumers-on-virtual-currencies, Accessed on 15.04.2020.
20. EBA, Report with advice for the European Commission, 09.01.2019, p. 12, Available at https://eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf?retry=1 , Accessed on 22.04.2020.
21. ECB, Lecture by Tommaso Padoa-SchioppaMember of the Executive Board of the European Central Bank, Washington D.C., 24.09.1999, Available at

https://www.ecb.europa.eu/press/key/date/1999/html/sp990924_1.en.html , Accessed on 25.04.2020.

22. EY, AML due diligence requirements from a Swiss banking perspective, Cryptocurrencies, September 2019, p. 4, Available at https://www.eycom.ch/en/Publications/20191001-Cryptocurrencies-AML-due-diligence-requirements-from-a-Swiss-banking-perspective/download, Accessed on 10.05.2020
23. EY, Why financial institutions need to focus on transparency, 12.07.2019, Available at https://www.ey.com/en_om/tax/why-financial-institutions-need-to-focus-on-transparency Accessed on 05.04.2020.
24. Electronic identification schemes notified pursuant to Article 9(1) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2019.425.01.0006.01.ENG&toc=OJ:C:2019:425:TOC#ntc1-C_2019425EN.01000601-E0001, Accessed on 09.05.2020.
25. EU-LISA, Perspectives for EU-LISA and the Large-scale IT Systems, Research and Technology Monitoring Report, 2019, Available at https://www.eulisa.europa.eu/Publications/Reports/DLTs%20and%20blockchain%20report.%20Dec%202019.pdf , Accessed 12.04.2020.
26. European Central Bank, Virtual currency schemes, October 2012, Available at https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf, Accessed on 13.04.2020.
27. European Commission, Blockchain Technologies, 15 January 2020, Available at https://ec.europa.eu/digital-single-market/en/blockchain-technologies, Accessed on 12.04.2020.
28. European Commission, Complexity of EU law in the domestic implementing process, Brussels, 03.07.2014, Available at https://ec.europa.eu/dgs/legal_service/seminars/20140703_baratta_speech.pdf , Accessed on 29.04.2020.
29. European Commission, What Is Hazard And Risk, Risk Assessment And Management, Available at https://ec.europa.eu/info/sites/info/files/file_import/better-regulation-toolbox-15_en_0.pdf, Accessed on 06.04.2020.
30. European Parliament, Cryptocurrencies and Blockchain, Legal context and implications for financial crime, money laundering and tax evasion, p. 20-22, Available at https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf , Accessed 10.04.2020.
31. European Parliament, Virtual currencies and terrorist financing: assessing the risks and evaluating responses, p. 27, Available at https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf , Accessed on 08.04.2020.
32. Executive Summary, National Money Laundering Risk Assessment, 2018, Available at https://home.treasury.gov/system/files/136/2018NMLRA_12-18.pdf , Accessed on 02.05.2020.

33. Fan, Zhang, The "Risk-Based" Principle of AML Management, 19.09.2017, Available at https://www.acamstoday.org/the-risk-based-principle-of-aml-management/, Accessed on 05.04.2020.

34. FATF, Financial Institutions, FATF Glossaries, Available at https://www.fatf-gafi.org/glossary/d-i/, Accessed on 23.04.2020.

35. FATF, Guidance for A Risk-Based Approach, The Banking Sector, 2014, Available at http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf, Accessed on 07.04.2020.

36. FATF, Guidance For A Risk-Based Approach, Virtual Currencies, p. 7, Available at https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf , Accessed on 24.04.2020.

37. FATF, Money Laundering through Money Remittance and Currency Exchange Providers, 2018, p. 21, Available at https://rm.coe.int/fatf-report-money-laundering-through-money-remittance-and-currency-exc/16807150ad , Accessed on 27.04.2020.

38. FATF, Virtual Currencies, Key Definitions and, Potential AML/CFT Risks, June 2014, Available at https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, Accessed on 10.04.2020.

39. FATF, Who we are, Available at https://www.fatf-gafi.org/about/ , Accessed on 06.04.2020.

40. Financial Intelligence Unit, Guidelines on the characteristics of suspicious transactions, Police and Border Guard Board, Available at https://www.politsei.ee/files/Rahapesu/juhend-kahtlaste-tehingute-tunnuste-kohta-en.pdf?3e4fc8c9fe, Accessed on 11.05.2020.

41. Financial Stability Board, Risk Appetite Definition, Principles for An Effective Risk Appetite Framework, Available at https://www.fsb.org/wp-content/uploads/r_131118.pdf, Accessed on 10.05.2020.

42. Financial Supervisory Authority, Article 4.1.3, Advisory Guidelines of Finantsinspektsioon "Organisational solutions and preventive measures for credit and financial institutions to take against money laundering and terrorist financing", p. 25, Available at https://www.fi.ee/sites/default/files/2019-01/FI%20rahapesu%20t%C3%B5kestamise%20juhend%202018%20%28EN%29_pdf.pdf , Accessed on 10.05.2020.

43. Financial Supervisory Authority, Which regulations apply to this activity, Information for entities engaging with virtual currencies and ICOs, Available at https://www.fi.ee/en/investment/aktuaalsed-teemad-investeerimises/virtuaalraha-ico/information-entities-engaging-virtual-currencies-and-icos , Accessed on 06.05.2020.

44. FINTRAIL, Assessing Risk, Cryptocurrencies: Getting Serious About Financial Crime Risk Management, A FINTRAIL White Paper, August 2018, Available at https://static1.squarespace.com/static/5b9798661aef1d8112a02bd0/t/5c0d5ad9562fa76785391c0b/1544379105284/Fintrail+Cryptocurrencies+WP+2018+280818.pdf , Accessed on 08.05.2020.

45. Fordham Law School, Virtual Currencies and the Challenges to Compliance Wednesday, Fordham/Accenture Compliance Series, 13.06.2018 p. 59, Available at

fordham.edu/download/downloads/id/10965/Accenture_Compliance_Virtual_Course_Materials.pdf

46. French Ministry of Economics, Annual report 2011, July 2012, p. 26, Available at https://www.economie.gouv.fr/files/2011_rapport_ang.pdf , Accessed on 14.04.2020.
47. Haeberli, Daniel, Stefan Oesterhelt, Alexander Wherlock, Switzerland, Blockchain & Cryptocurrency Regulation 2020, Available at https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/switzerland, Accessed on 13.05.2020.
48. Hāka, Žanete, Latvijas Banka un FKTK: Bitcoin nav ne valūta, ne maksāšanas līdzeklis, 23.07.2014, Available at https://www.db.lv/zinas/latvijas-banka-un-fktk-bitcoin-nav-ne-valuta-ne-maksasanas-lidzeklis-417958, Accessed on 19.04.2020.
49. He, Dong, Karl Habermeier, Ross Leckow, Vikram Haksar, Yasmin Almeida, Mikari Kashima, Nadim Kyriakos-Saad, Hiroko Oura, Tahsin Saadi Sedik, Natalia Stetsenko, and Concepcion Verdugo-Yepes, Virtual Currencies and Beyond: Initial Considerations, January 2016, p. 17, Available at https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf, Accessed on 17.04.2020.
50. Hudak, Steve, FinCEN Names ABLV Bank of Latvia an Institution of Primary Money Laundering Concern and Proposes Section 311 Special Measure, 13.02.2018, Available at https://www.fincen.gov/news/news-releases/fincen-names-ablv-bank-latvia-institution-primary-money-laundering-concern-and, Accessed on 05.04.2020.
51. Intelligence Unit, Available at https://www.politsei.ee/files/Rahapesu/rahapesu-andmebueroole-esitatava-teate-esitamise-juhend-en.pdf?eead45cee2 , Accessed on 11.05.2020.
52. International Centre for Asset Recovery, Basel AML Index 2019 A country ranking and review of money laundering and terrorist financing risks around the world, August 2019, Available at https://www.baselgovernance.org/sites/default/files/2019-08/Basel%20AML%20Index%202019.pdf, Accessed on 02.05.2020.
53. International Monetary Fund, Assessing Financial System Integrity—Anti-Money Laundering and Combating the Financing of Terrorism, Financial Sector Assessment: A Handbook, Chapter 8, p. 207, Available at https://www.imf.org/external/pubs/ft/fsa/eng/pdf/ch08.pdf, Accessed on 05.04.2020.
54. International Standards On Combating Money Laundering and The Financing of Terrorism & Proliferation The FATF Recommendations updated June 2019, Recommendation No. 10
55. Jensen, Teis, Explainer: Danske Bank's 200 billion euro money laundering scandal, Reuters, 19.11.2018, Available at https://www.reuters.com/article/us-danske-bank-moneylaundering-explainer/explainer-danske-banks-200-billion-euro-money-laundering-scandal-idUSKCN1NO10D, Accessed on 07.05.2020.
56. Kirkpatrick, Grant, The Corporate Governance Lessons from the Financial Crisis, OECD, 2009, p. 26, Available at https://www.oecd.org/finance/financial-markets/42229620.pdf, Accessed on 05.05.2020.
57. Kirschenbaum, Joshua, German Marshall Fund of the United States, Report, 2018, Available at www.jstor.org/stable/resrep18827, Accessed on 05.04.2020.

58. KPMG, Cross border cryptocurrency compliance, p. 9, Available at https://advisory.kpmg.us/content/dam/advisory/en/pdfs/cross-border-cyryptocurrency-compliance.pdf , Accessed on 05.05.2020.

59. Leckow, Ross, Virtual currencies: the regulatory challenges, p. 137, Available at https://ccl.yale.edu/sites/default/files/files/Leckow_Ross_Virtual%20currencies%20-%20the%20regulatory%20challenges.pdf , Accessed on 02.05.2020.

60. Lehemets, Maarja, New crypto rules – stricter requirements for virtual currency service providers in Estonia, 05.03.2020, Available at https://triniti.eu/2020/03/05/new-crypto-rules-stricter-requirements-for-virtual-currency-service-providers-in-estonia/, Accessed on 12.05.2020.

61. Lextal, The Estonian crypto regulation faces a lethal challenge, Available at https://lextal.ee/en/the-estonian-crypto-regulation-faces-a-lethal-challenge/, Accessed on 09.05.2020.

62. Loboda, Kristīna, Sliekšņa deklarācijas – kam un kā tās būs jāiesniedz, 02.12.2019, Available at https://lvportals.lv/skaidrojumi/311016-slieksna-deklaracijas-kam-un-ka-tas-bus-jaiesniedz-2019, Accessed on 05.05.2020.

63. Mckinsey&Company, Why anti-money laundering should be top priority for financial institutions, Available at https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/banking%20blog/why%20aml%20should%20be%20a%20top%20priority%20for%20financial%20institutions/why-aml-should-be-a-top-priority-for-financial-institutions.ashx, Accessed on 05.04.2020.

64. Minister of the Interior, Guidelines for Submitting A Report To The Financial

65. Moy, Jamie, Forget Bitcoin, It's All About The Blockchain, Forbes, 22.02.2018, Available at https://www.forbes.com/sites/jamiemoy/2018/02/22/forget-bitcoin-its-all-about-the-blockchain/#2d12f04b5f6b, Accessed on 25.04.2020.

66. MONEYVAL, Anti-money laundering and counter-terrorist financing measures Latvia Fifth Round Mutual Evaluation Report, 2018, p. 104, Available at https://rm.coe.int/moneyval-2018-8-5th-round-mer-latvia/16808ce61b, Accessed on 28.04.2020.

67. Novak, Nejc, EU Introduces Crypto Anti-Money Laundering Regulation, 02.01.2018, Available at https://medium.com/@nejcnovaklaw/eu-introduces-crypto-anti-money-laundering-regulation-d6ab0ddedd3, Accessed 22.04.2020.

68. Noziedzīgi iegūtu līdzekļu legalizācijas novēršanas dienests, Virtuālās Valūtas Noziedzīgi Iegūtu Līdzekļu Legalizācijas Un Terorisma Finansēšanas Riski, Available at https://www.fid.gov.lv/images/Downloads/useful/Riska_nov_virt_valutas_LV.pdf , Accessed on 01.05.2020.

69. OECD, Economic Survey of Estonia (December 2019), p. 4, Available at https://www.oecd.org/economy/estonia-economic-snapshot/ ,Accessed on 05.05.2020.

70. OECD, The Policy Environment for Blockchain Innovation and Adoption 2019 OECD Global Blockchain Policy Forum Summary Report, Available at https://www.oecd.org/finance/2019-OECD-Global-Blockchain-Policy-Forum-Summary-Report.pdf, Accessed on 13.04.2020.

71. Police and Border Guard Board, Cross Border Operation, Activity licence for the provision of financial services, Available at https://www.eesti.ee/en/licences-and-notices-of-economic-

activity/financial-activities/activity-licence-for-the-provision-of-financial-services/ , Accessed on 07.05.2020.

72. Poskriarov, Fedor, Maria Chiriaeva, Christope Cavin, Managing AML compliance risks, Blockchain and Cryptocurrency Regulation 2020, Cryptocurrency compliance and risks: A European, KYC/AML Perspective, Available at https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/11-cryptocurrency-compliance-and-risks-a-european-kyc-aml-perspective , Accessed 01.05.2020.
73. Putniņš, Pēters, ABLV Bank AS licence ir anulēta, bankas pašlikvidācija norit FKTK uzraudzībā, FKTK, 12.07.2018, Available at https://www.fktk.lv/jaunumi/pazinojumi-medijiem/peters-putnins-ablv-bank-as-licence-ir-anuleta-bankas-paslikvidacija-norit-fktk-uzraudziba/, Accessed on 05.04.2020.
74. Rahapesu ja terrorismi rahastamise tõkestamise valitsuskomisjoni analüüs ja ettepaneku, 2018, p. 14, Available at https://www.rahandusministeerium.ee/sites/default/files/rahapesu_tokestamise_valitsuskomisjoni_analuus_ja_ettepanekud.pdf, Accessed on 07.05.2020.
75. State Revenue Service, Virtuālās valūtas maiņas pakalpojumu sniedzēji, Available at https://www.vid.gov.lv/sites/default/files/2_8_virtualas_valutas_mainas_pakalpojumu_sniedzeji.pdf, Accessed on, 30.04.2020.
76. The European Union Blockchain Observatory And Forum, Legal And Regulatory Framework Of Blockchains And Smart Contracts, Available at https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf, Accessed 12.04.2020.
77. The Wolfsberg Group, Appendix C: Example Client Inherent Risk Ratings, The Wolfsberg Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption, Available at https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/faqs/17.%20Wolfsberg-Risk-Assessment-FAQs-2015.pdf , Accessed on 08.04.2020.
78. Thompson Reuters, Latvia, Cryptocurrencies by country, 25 Oct 2017, Available at https://blogs.thomsonreuters.com/answerson/world-cryptocurrencies-country/, Accessed on 19.04.2020.
79. Thomson Reuters, 5 questions that can help reduce the regulatory burden on compliance officers, Available at https://legal.thomsonreuters.com/en/insights/articles/reducing-regulatory-burden-on-compliance-officers Accessed on 05.04.2020.
80. U.S. Department of Justice Federal Bureau of Investigation Money laundering, Forfeiture and Bank Fraud Unit, What Is a Money Mule, Money Mule Awareness, Available at https://www.fbi.gov/file-repository/money-mule-awareness-booklet.pdf , Accessed on 02.05.2020.
81. UNODC, Virtual Currencies, p. 95, Available at https://www.imolin.org/pdf/UNODC_VirtualCurrencies_final_EN_Print.pdf , Accessed on 02.05.2020.

82. Valsts ieņēmumu dienests, Par darījumiem ar kriptovalūtu un nodokļiem, 08.06.2017, Available at https://lvportals.lv/e-konsultacijas/11918-par-darijumiem-ar-kriptovalutu-un-nodokliem-2017, Accessed on 19.04.2020.
83. Virtual currency schemes – a further analysis, February 2015, Available at https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, Accessed on 16.04.2020.